大学数学 スポットライト・シリーズ ❶

シローの定理

佐藤隆夫 著

近代科学社

◆ 読者の皆さまへ ◆

小社の出版物をご愛読くださいまして，まことに有り難うございます．

おかげさまで，㈱近代科学社は 1959 年の創立以来，2009 年をもって 50 周年を迎えることができました．これも，ひとえに皆さまの温かいご支援の賜物と存じ，衷心より御礼申し上げます．

この機に小社では，全出版物に対して UD（ユニバーサル・デザイン）を基本コンセプトに掲げ，そのユーザビリティ性の追究を徹底してまいる所存でおります．

本書を通じまして何かお気づきの事柄がございましたら，ぜひ以下の「お問合せ先」までご一報くださいますようお願いいたします．

お問合せ先：reader@kindaikagaku.co.jp

なお，本書の制作には，以下が各プロセスに関与いたしました：

・企画：小山　透
・編集：小山　透，石井沙知
・組版 (TeX)・印刷・製本・資材管理：藤原印刷
・カバー・表紙デザイン：菊池周二
・広報宣伝・営業：冨髙琢磨，山口幸治

大学数学 スポットライト・シリーズ
刊行の辞

周知のように，数学は古代文明の発生とともに，現実の世界を数量的に明確に捉えるために生まれたと考えられますが，人類の知的好奇心は単なる実用を越えて数学を発展させて行きました．有名なユークリッドの『原論』に見られるとおり，現実的必要性をはるかに離れた幾何学や数論，あるいは無理量の理論がすでに紀元前 300 年頃には展開されていました．

『原論』から数えても，現在までゆうに 2000 年以上の歳月を経るあいだ，数学は内発的な力に加えて物理学など外部からの刺激をも様々に取り入れて絶え間なく発展し，無数の有用な成果を生み出してきました．そして 21 世紀となった今日，数学と切り離せない数理科学と呼ばれる分野は大きく広がり，数学の活用を求める声も高まっています．しかしながら，もともと数学を学ぶ上ではものごとを明確に理解することが必要であり，本当に理解できたときの喜びも大きいのですが，活用を求めるならばさらにしっかりと数学そのものを理解し，身につけなければなりません．とは言え，発展した現代数学はその基礎もかなり膨大なものになっていて，その全体をただ論理的順序に従って粛々と学んでいくことは初学者にとって負担が大きいことです．

そこで，このシリーズでは各巻で一つのテーマにスポットライトを当て，深いところまでしっかり扱い，読み終わった読者が確実に，ひとまとまりの結果を理解できたという満足感を得られることを目指します．本シリーズで扱われるテーマは数学系の学部レベルを基本としますが，それらは通常の講義では数回で通過せざるを得ないが重要で珠玉のような定理一つの場合もあれば，ε-δ 論法のような，広い分野の基礎となっている概念であったりします．また，応用に欠かせない数値解析や離散数学，近年の数理科学における話題も幅広く採り上げられます．

本シリーズの外形的な特徴としては，新しい製本方式の採用により本文の余白が従来よりもかなり広くなっていることが挙げられます．この余白を利用して，脚注よりも見やすい形で本文の補足を述べたり，読者が抱くと思われる疑問に答えるコラムなどを挿入して，親しみやすくかつ理解しやすものになるよういろいろと工夫をしていますが，余った部分は読者にメモ欄として利用していただくことも想定しています．

また，本シリーズの編集幹事は東京理科大学の教員から成り，学内で活発に研究教育活動を展開しているベテランから若手までの幅広く豊富な人材から執筆者を選定し，同一大学の利点を生かして緊密な体制を取っています．

本シリーズは数学および関連分野の学部教育全体をカバーする教科書群ではありませんが，読者が本シリーズを通じて深く理解する喜びを知り，数学の多方面への広がりに目を向けるきっかけになることを心から願っています．

編集幹事一同

まえがき

きわめて率直にいえば，群とは何かしらの演算（足し算でも掛け算でもよい）を一つ持つような集合のことである．例えば，整数全体は足し算に関する群であり，零以外の実数全体は掛け算に関する群をなす．これらは最も身近な群の例である．現代数学においては，このような馴染み深い例以外にも抽象的な群が数多く現れ，重要な役割を果たしている．

19 世紀に，ガロアが多項式の根たちの置換のなす群と数体との密接な関係に注目したことによって花開いたガロア理論は，定規とコンパスによる作図可能性の問題や，四則演算と累乗根による代数方程式の可解性の問題への応用にとどまらず，代数的整数論や数論幾何学などとも深く関わり合いながら非常に高度な理論に発展している．

一方で，1872 年にクラインがエルランゲン大学で行った教授への就任演説の中で，「幾何学とは変換群によって保たれる空間を研究する学問である」と説いているように，古典的にもかなり早い時期から群と幾何学との関連性も指摘されている．

さらに，位相幾何学（トポロジーともいう）的な観点からより具体的な例を挙げれば，種々の位相空間（特に低次元位相幾何学と呼ばれる分野では，可微分多様体や，CW 複体などの構造を持つものが盛んに研究されている）の位相不変量として基本群やホモロジー群などが定義され，これらの群は空間が持つ幾何学的な情報を代数的に記述するための道具としてきわめて有益である．このような例以外にも，群論は現代数学の様々な分野で用いられており，その有用性については論をまたない．

さて，群論における最も重要な問題のうちの一つは，群の同型類を決定する問題であろう．すなわち，与えられた二つの群が，単なる集合としてではなく演算の性質も含めた意味で同じものとみなせるかどうかということを問う問題である．これは一般に，非常に難

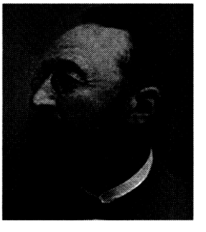
しい．まず，ひとえに群全部を考えるのではあまりに多様すぎるので，考察する対象に応じてしばしばある条件に制限した群の族を考える．例えば，群の要素の数に注目して無限群か有限群か，群の生成元に注目して有限生成か無限生成か，また群の演算の可換性を考えて可換群か非可換群か，などである．

しかしながら，そのような群の族に限ったとしても，異なる構造を持つ群は山ほどある．有限生成アーベル群のように理論上は同型類を完全に分類できるような場合もあるが，一般には，条件をいくつか付した群であっても，群の構造を明確に記述するのはきわめて困難である．これは有限群の族においても例外ではない．

そのような状況の下，与えられた有限群が素数冪位数の部分群をどの程度有するかということを，その存在と個数についてかなり明示的な言及をする**シローの定理**は，すべての有限群に対して適用できる汎用性の高い定理であり，応用上も非常に有益である．シローの定理は 1872 年にシロー[1] が[16] において証明し，それ自身は古典的なものではあるが，その後の群論の発展とも相まって多くの別証明などが与えられ，現在ではかなり整備されたものになっている．初等的な群論の事実をいくつも織り交ぜながら証明が進み，多くの具体例に適用が可能であるので，初学者にとっては学びがいのある格好の題材でもある．我々が本書でシローの定理にスポットライトを当てて解説する理由はここにある．

一般に，群論は微分積分学や幾何学と比べると非常に抽象的な理論である．このようなものを咀嚼して理解を深めるにあたり最も重要なことは，多くの具体例を頭の中に思い描き，新しい概念が出てくるごとにそれらの例に適用して確認することである．抽象的で，なぜそのようなことを思いついたのかさえもよく分からない定理であっても，具体例に適用させてみれば自然に成り立ちそうなものであることが意外と容易に理解できたりすることもある．しかしながら一方で，手持ちの例が特殊で限られたものであると，かえって直観が鈍ってしまうこともある．ある例では当たり前のように成り立つ性質が，別の例ではまったく成り立たないなどということはよくあることである．初学者のうちはまず簡単な例を中心に着実に理論を理解することが肝要であるが，慣れてきたら貪欲に幅広い文献にも触れて自分が自在に扱える群の例を増やしていくことをお勧めする．

[1] Peter Ludwig Mejdell Sylow（1832. 12. 12. – 1918. 9. 7.）



ノルウェーの数学者．1858 年から 40 年間，ノルウェーの Frederikshald（現 Halden）で高校教師をしていた．1862 年から王立フレデリック大学（現オスロ大学）で代用講師としてガロア理論の講義を行い，1898 年に同大教授に任命された．王立フレデリック大学は 1939 年にオスロ大学と改名され，1946 年までノルウェーで唯一の大学であった．現在，オスロ大学はノルウェーで最も古い大学であり，北欧で最も名門とされる大学のうちの一つである．

本書では主に有限群を扱うが，特に巡回群，対称群，正二面体群，交代群については，生成元，中心，アーベル化，および共役類に関する内容を（演習問題も含め）すべて記述した．また，種々の概念を解説する際に，その利便性や有益性などを考慮して上記の有限群以外にも，一般線型群[2] や特殊線型群，有理整数環上のハイゼンベルグ群などの無限群も多少取り扱った．

通常，論文などの出版物で同じような証明を行う場合，「上の議論と同様」などの言葉で省略しがちであるが，本書では反復学習という意を込めてなるべく繰り返して説明するよう心掛けた．したがって，読者が本書を読み終えるころには，群論でよく用いられる概念，手法等に関してはかなりくどく感じるかもしれない．群論に限ったことではないが，より高度な数学の理論を学ぶに当たり，その基礎となる概念に関しては，自由自在に使いこなせるようになっていなければ，ちょっとしたことでも太刀打ちできなくなり，結果として以前のノートや教科書をひっぱり出してきてぶつぶつと格闘し多大な時間を費やすことになる．このような経験も大切ではあるが，避けられるのであれば，極力避けたい．その方がより楽しみながらスムーズに数学を進めることができ，結果として勉強研究がはかどり，精神衛生面においてもよいと思う．そのためには，基本的なことを如何に着実に身に着けているかということが大事である．本書で初めて群論に触れた読者の方々が，本書を読み終えるころに，「この本は説明がくどすぎる」，「当たり前なことが何度も書いてある」等と思っていただけたら，著者として大変嬉しく思う次第である．

2) 「線型」は「線形」と書かれることもあるが，これは linear type の訳語であるので本書では「線型」を採用することにする．

謝辞

今回，若輩の私に本の執筆という貴重な機会を与えてくださった，東京理科大学理学部第二部数学科の宮岡悦良先生，および同理学部第一部数学科の眞田克典先生に心から感謝いたします．特に，眞田克典先生，および同理学部第一部数学科の功刀直子先生には，お忙しい中拙著の草稿に目を通していただきました．この場を借りて深くお礼を申し上げます．近代科学社社長の小山透さんは何度も研究室に足を運んで下さり，本シリーズの趣旨や構成などについて大変丁寧に説明していただきました．著者の遅々として進まない作業に，顔色一つ変えることなくいつも笑顔で親切にご対応頂いたお人柄に

支えられました．また，同社の高山哲司さんと石井沙知さんには原稿の校正に際し，何度も誠実で丁寧にご対応いただきました．近代科学社の皆様に改めて深謝致します．本書では後に掲げる文献を大いに参考にさせていただきました．本文中では逐一出典を明示することはしませんでしたが，これらの本の執筆者に敬意を表すとともに深く感謝いたします．最後に，この本の出版を心待ちにしてくれていた，長崎で古書店を営む父に本書を捧げたいと思います．

東京 神楽坂にて
2015 年 2 月　　佐　藤　隆　夫

記号の準備

本書を通じて以下の記号[3]や言葉遣いは断りなしに用いるので注意されたい．

$$\mathbb{N} := \text{自然数全体の集合} = \{1, 2, 3, \ldots\}$$

$$\mathbb{Z} := \text{整数全体の集合} = \{0, \pm1, \pm2, \pm3, \ldots\}$$

$$\mathbb{Q} := \text{有理数全体の集合}$$

$$\mathbb{R} := \text{実数全体の集合}$$

$$\mathbb{C} := \text{複素数全体の集合}$$

整数 $a, b \in \mathbb{Z}$ に対して，ある整数 $q \in \mathbb{Z}$ が存在して $a = bq$ となるとき，a は b の倍数，もしくは b は a の約数という．このとき，$b|a$ と書く．例えば，$3|(-15)$ であり，$(-4)|8$ である．0 でない整数 m, n に対して m と n の最大公約数を $\gcd(m, n)$ と表す．

[3] $:=$ は記号などを定義するときに用いる等号である．例えば，A を B で定義するとき，$A := B$ のように用いる．

目　次

1 群の定義と例

この章では，用語の準備も兼ねて，群の定義や諸性質を解説する．特に，多くの例を通して群の性質を深く理解して群論の手法に慣れていただきたい．

1.1 群の定義

定義 1.1 (群) 集合 G の各元 $\sigma, \tau \in G$ に対して，σ と τ の**積** (product) と呼ばれる元 $\sigma \cdot \tau \in G$ が一意的に定義されていて，これが以下の三つの性質[4] を満たすとき G は**群** (group) であるという．

(G1) **(結合法則)** 任意の $\sigma, \tau, \rho \in G$ に対して，$(\sigma \cdot \tau) \cdot \rho = \sigma \cdot (\tau \cdot \rho)$ が成り立つ．

(G2) **(単位元の存在)** ある $e \in G$ が存在して，任意の $\sigma \in G$ に対して，

$$e \cdot \sigma = \sigma \cdot e = \sigma$$

が成り立つ．このとき，e を G の**単位元** (unit) という．本書では簡単のため主に，1_G または単に 1 と表す．

(G3) **(逆元の存在)** 任意の $\sigma \in G$ に対して，ある $\sigma' \in G$ が存在して，

$$\sigma \cdot \sigma' = \sigma' \cdot \sigma = e$$

となる．このとき，σ' を σ の**逆元** (inverse) といい，σ^{-1} と表す．

積を表す記号 $\cdot$ は，前後の文脈から明らかに意味が分かるときや，他の記号と合わせて複雑になるときなどは省略して，$\sigma\tau$ などと表す[5]．

4) 「何だ，たった三つか．」と思われるかもしれないが，逆にいえばたった三つしかないからこそ考えうる対象の幅が大きく広がり，これだけのことから実に多くの豊かで有益な理論が展開される．

5) 以下特に断らない限り，群の積は省略形で表す．

また，群の積は**乗法** (multiplication) と呼ばれることもある．

定義 1.2 (**アーベル群**) 群 G の任意の元 $\sigma, \tau \in G$ に対して $\sigma\tau = \tau\sigma$ が成り立つとき，G の積は可換であるといい，G のことを**可換群** (commutative group)，もしくは**アーベル群** (abelian group) [6] という．群がアーベル群でないとき**非可換群** (noncommutative group) とか，**非アーベル群** (non-abelian group) などと呼ぶ．

[6] 通常，abelian の頭文字は小文字で書かれる．

アーベル群においては，（すべての場合ではないが）慣習的に積の記号 $\cdot$ を $+$ で表すことがある．すなわち，$\sigma \cdot \tau$ を $\sigma + \tau$ と表す．このとき，群の単位元 e を 0 と表し，$\sigma \in G$ の逆元を $-\sigma$ と表す[7]．この場合のアーベル群の積は乗法と呼ぶ代わりに**加法** (addition) と呼ばれる．

[7] σ の**マイナス元**と呼ぶこともある．

注意 1.3 群は，積が乗法的，または加法的に書かれているかによってそれぞれ，**乗法群** (multiplicative group)，または**加法群** (additive group) と呼ばれる．

例 1.4 (1) 整数全体の集合 $\mathbb{Z}$ において，通常の足し算 $+$ を考えるとこれは加法群になる．実際，結合法則が成り立つことはほぼ明らかであろう．また，単位元，および整数 n の逆元はそれぞれ，通常の 0，および $-n$ で与えられる．また，任意の整数 m, n に対して，$m + n = n + m$ となることも明らか[8]．

(2) 実数全体の集合 $\mathbb{R}$ から 0 を除いた集合を $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$ とおく．すると，$\mathbb{R}^\times$ は通常の実数の積に関して乗法群になる．この場合も，結合法則については明らかであろう．単位元，および実数 r の逆元はそれぞれ，通常の 1，および $1/r$ である．また明らかに，任意の $r, s \in \mathbb{R}$ に対して $rs = sr$ が成り立つので，$\mathbb{R}^\times$ はアーベル群である．しかしながらこの場合，紛らわしいので積を加法的に書くことはない．

(3) (2) の一般化を考えよう．可換環[9] R に対して，R の乗法単位元を 1_R とする．$u \in R$ に対して，ある元 $v \in R$ で $uv = 1_R$ となるものが存在するとき u を R の**単元** (unit)，または**可逆元** (invertible element) という[10]．可換環 R の単元全体の集合を $R^\times$ とおくと，$R^\times$ は R の乗法によって乗法群となる．こ

[8] 保育園に通う娘に 5 足す 4 はいくつ？と聞いたら（指折りで）9 と答えたので，4 足す 5 はいくつと聞いたらまた指折りで数えはじめた．整数の加法の可換性もあまり自明ではないのかもしれない．

[9] 率直にいえば，可換環とは加法群であって，任意の 2 元が交換可能な乗法が定義されている集合．特に，体は可換環である．本書では特に断らない限り，環といえば単位的結合可換環を表すことにする．よく分からない場合は，$R = \mathbb{Z}$ の場合を想像して頂ければ十分である．

[10] 一般に，可換環において単元とは，乗法単位元のみを指すわけではないことに注意せよ．

れを R の**単元群** (group of units) という.

注意 1.5 G をアーベル群とし, $a, b \in G$ とする. 任意の整数 m に対して, $(ab)^m = a^m b^m$ が成り立つ（帰納法を用いて容易に示される）. G が非可換群のとき, この式は一般には成り立たない.

次に, 群 G の単位元と, 各元の逆元の一意性について述べる.

定理 1.6 G を群とする. このとき, 以下が成り立つ.

(1) 任意の $\sigma \in G$ に対して, $\sigma e = e\sigma = \sigma$ を満たす $e \in G$ は一意的である.

(2) 任意の $\sigma \in G$ に対して, $\sigma\sigma' = \sigma'\sigma = e$ を満たす $\sigma' \in G$ は一意的である.

証明. (1) 任意の $\sigma \in G$ に対して, $e' \in G$ も $\sigma e' = e'\sigma = \sigma$ を満たすとする. このとき, $e = e'$ を示せばよい. すると, e' が単位元の性質を満たすから $e = ee'$ であり, e も単位元の性質を満たすから $ee' = e'$ である. ゆえに, $e = ee' = e'e = e'$ を得る.
(2) 任意の $\sigma \in G$ に対して, $\sigma'' \in G$ も $\sigma\sigma'' = \sigma''\sigma = e$ を満たすとする. このとき, $\sigma' = \sigma''$ を示せばよい. すると,

$$
\begin{aligned}
\sigma' &= \sigma' e && \text{（単位元の性質）} \\
&= \sigma'(\sigma\sigma'') && \text{（上の仮定）} \\
&= (\sigma'\sigma)\sigma'' && \text{（結合法則）} \\
&= e\sigma'' && \text{（上の仮定）} \\
&= \sigma'' && \text{（単位元の性質）}
\end{aligned}
$$

となるので, 求める結果を得る. □

定義 1.7（位数） 群 G に対して, G に含まれる要素の数を G の**位数** (order) といい, $|G|$ と表す[11]. 群 G は, $|G| < \infty$ のとき**有限群** (finite group), $|G| = \infty$ のとき**無限群** (infinite group) という.

11) 一般に, 集合 X に対して X に含まれる要素の数を $|X|$ と書く. X が無限集合のとき, $|X|$ は X の濃度を表す.

例 1.8 $n \geq 1$ を自然数とし, 1 の n 乗根全体の集合を

$$\mathcal{U}_n := \left\{ \exp\left(\frac{2k\pi\sqrt{-1}}{n} \right) \middle| \, 0 \leq k \leq n-1 \right\}$$

とおく．ここで，$\exp z$ は複素指数関数[12] を表し，特に

$$\exp\left(\frac{2k\pi\sqrt{-1}}{n}\right) = \cos\left(\frac{2k\pi}{n}\right) + \sqrt{-1}\sin\left(\frac{2k\pi}{n}\right)$$

である[13]．$\mathcal{U}_n$ は $\mathbb{C}$ の部分集合である．そこで，複素数の通常の乗法を考えることにより，$\mathcal{U}_n$ は乗法的アーベル群になる．実際，$\mathcal{U}_n$ に積が定義されることは以下のようにして分かる．任意の $\exp(\frac{2k\pi\sqrt{-1}}{n}), \exp(\frac{2l\pi\sqrt{-1}}{n}) \in \mathcal{U}_n$ に対して，これらの積が $\mathcal{U}_n$ に属していることを確かめればよい．すると，$k+l$ を n で割った商を q，余りを m とおくと，$0 \leq m \leq n-1$ であり，$k+l = nq+m$ と書ける．このとき，

$$\begin{aligned}\exp\left(\frac{2k\pi\sqrt{-1}}{n}\right)\exp\left(\frac{2l\pi\sqrt{-1}}{n}\right) &= \exp\left(\frac{2(k+l)\pi\sqrt{-1}}{n}\right)\\ &= \exp\left(\frac{2(nq+m)\pi\sqrt{-1}}{n}\right)\\ &= \exp\left(\frac{2m\pi\sqrt{-1}}{n} + 2q\pi\sqrt{-1}\right)\\ &= \exp\left(\frac{2m\pi\sqrt{-1}}{n}\right) \in \mathcal{U}_n\end{aligned}$$

となり，$\mathcal{U}_n$ に積が定義されていることが分かる．この積が結合法則を満たし，かつ可換であることは，複素数の積がそれらを満たすことから明らかである．また，単位元，および $\exp\left(\frac{2k\pi\sqrt{-1}}{n}\right)$ の逆元はそれぞれ，$1 = \exp(0), \exp\left(\frac{2k'\pi\sqrt{-1}}{n}\right)$ で与えられる．ここで，$0 \leq k' \leq n-1$ は，$-k$ を n で割ったときの余りである．ゆえに，$\mathcal{U}_n$ は乗法的アーベル群になることが分かる．明らかに，$|\mathcal{U}_n| = n$ であるから $\mathcal{U}_n$ は有限群である．

例 1.9 $K = \mathbb{Q}, \mathbb{R}$ または $\mathbb{C}$ とする[14]．K の元を成分とする 2 次正方行列全体の集合を $M(2,K)$ とおく．$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2,K)$ に対して，

$$\det A = ad - bc \in K$$

を A の**行列式** (determinant) という[15]．$A,\ B \in M(2,K)$ に対して，

$$\det(AB) = (\det A)(\det B) \tag{1.1}$$

12) 中学高等学校の教科書では，「かんすう」は関数と書かれるが元々は函数と書かれた．その理由としては，英語の「function」を中国語で表す際に「函」の音読みが function の発音に近かったことや，「函」は「箱」に通じており，関数の本質であるブラックボックスを意味する漢字として適していることなど，諸説あるようである．現代でも「函数」という表記は頻繁に用いられるが，本書は初学者向けの入門書でもあり，あまりわずらわしい思いをしなくてすむように「関数」を用いることにする．

13) 指数関数として e^z と書くほうが慣れているかもしれないが，e は単位元などの記号で用いることがあることや，指数が複雑な式になると分かりづらいので $\exp z$ と表すことにする．

14) 実は，K は体（四則演算が入っている集合で，乗法は可換なもの）であれば何でもよい．よく分からないという方は $K = \mathbb{R}$ と思っても何ら問題ない．

15) 元来，行列式は連立一次方程式の解を決定するものという意味から，Gauss によってドイツ語で Determinante と名づけられた．「行列式」という訳語は明治期に高木貞治によって与えられたものである．

が成り立つ[16]．このとき，

$$\mathrm{GL}(2,K) := \{A \in M(2,K) \mid \det A \neq 0\}$$

とおくと，これは通常の行列の積に関して乗法群になる．実際，$\mathrm{GL}(2,K)$ に積が定義されることを確かめるには，任意の $A, B \in \mathrm{GL}(2,K)$ に対して，これらの積が $\mathrm{GL}(2,K)$ に属していることを確かめればよい．すると，(1.1) より，$\det A \neq 0$，$\det B \neq 0$ であれば $\det(AB) \neq 0$ であるので，$AB \in \mathrm{GL}(2,K)$ である．この積が結合法則を満たすことは，一般に 2 正方行列の積がそれを満たすことから明らか．また，単位元，および $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ の逆元はそれぞれ，

$$E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A^{-1} = \frac{1}{\det A}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

で与えられる．この $\mathrm{GL}(2,K)$ を K 上の 2 次の**一般線型群** (general linear group) という．任意の $a \in K \setminus \{0\}$ に対して，

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2,K)$$

であるから，K が無限集合のとき（例えば，$K = \mathbb{Q}, \mathbb{R}$ または $\mathbb{C}$ のとき），$\mathrm{GL}(2,K)$ は無限群である．

[16] 後述するように，n 次正方行列に対しても行列式が定義され，同様の等式が成り立つ．置換の性質を利用して証明されるが，2 次正方行列の場合はゴリ押しの計算でも確認できる．

1.2 群の例

この節では，これまでに挙げた例の外に，本書でも今後よく用いる群をいくつか紹介する．前節における例は，高校数学でも扱ったようなことを用いて構成されたが，以下では大学数学で初めて目にするような群も多く登場する．

1.2.1 対称群

n 個の文字 $1, 2, \ldots, n$ の集合を

$$X = \{1, 2, \ldots, n\}$$

とおく．写像 $\sigma : X \to X$ が

$$\{\sigma(1), \sigma(2), \ldots, \sigma(n)\} = \{1, 2, \ldots, n\}$$

を満たすとき，すなわち，$\sigma(1), \sigma(2), \ldots, \sigma(n)$ が $1, 2, \ldots, n$ を並べ換えたものであるとき，σ を X の**置換** (permutation) という．明らかに，X の置換は全部で $n!$ 個ある．σ は

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \tag{1.2}$$

とも表す．（これは**行列ではないことに注意されたい**）文字 $1, 2, \ldots, n$ の中に σ によって動かされない文字がある場合はその文字を省略することもある．また，この記号は $1, 2, \ldots, n$ の各元が σ によってどの元に写されるかを示すにすぎないので，σ によって写される元がきちんと対応していれば，上段は $1, 2, \ldots, n$ の順に並んでいなくてもよいものとする．すなわち，(1.2) の左辺に置いて適当に列を入れ換えたものはすべて同じものとみなす．例えば，$n = 4$ のとき

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} &= \begin{pmatrix} 4 & 3 & 2 & 1 \\ 1 & 4 & 2 & 3 \end{pmatrix} && \text{（列の入れ換え）} \\ &= \begin{pmatrix} 1 & 3 & 4 \\ 3 & 4 & 1 \end{pmatrix} && \text{（2 を省略）} \\ &= \begin{pmatrix} 4 & 3 & 1 \\ 1 & 4 & 3 \end{pmatrix} && \text{（列の入れ換え）} \end{aligned}$$

となる．

X の置換全体の集合を $\mathfrak{S}_n$ で表す[17]．任意の $\sigma, \tau \in \mathfrak{S}_n$ に対して，合成写像

$$\sigma \circ \tau : X \to X$$

はまた X の置換である．$\sigma \circ \tau$ は，X の各元を τ にしたがって並べ換えたものを，続けて σ にしたがって並べ換える写像である．そこで，これを $\mathfrak{S}_n$ における σ と τ の積と定め，単に $\sigma\tau$ と表す．

上で定めた，$\mathfrak{S}_n$ の積は，写像の合成であるから結合法則を満たす．実際，任意の $\sigma, \tau, \mu \in \mathfrak{S}_n$ および，任意の $i \in X$ に対して，

[17] $\mathfrak{S}$ はドイツ装飾大文字の S．ドイツ装飾文字はフラクトゥールともよばれ，神聖ローマ皇帝マクシミリアン 1 世の時代につくられた歴史がある．

$$((\sigma \circ \tau) \circ \mu)(i) = (\sigma \circ \tau)(\mu(i)) = \sigma(\tau(\mu(i)))$$
$$(\sigma \circ (\tau \circ \mu))(i) = \sigma((\tau \circ \mu)(i)) = \sigma(\tau(\mu(i)))$$

となるので，$((\sigma \circ \tau) \circ \mu) = (\sigma \circ (\tau \circ \mu))$ である．すなわち，$(\sigma\tau)\mu = \sigma(\tau\mu)$ となる．また，X のどの元も動かさない置換

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

のことを**恒等置換** (identity permutation) [18] といい，$1_{\mathfrak{S}_n}$ と表す．すると，任意の元 $\sigma \in \mathfrak{S}_n$ に対して，

$$1_{\mathfrak{S}_n}\sigma = \sigma 1_{\mathfrak{S}_n} = \sigma$$

となるのは明らかである．さらに，任意の $\sigma \in \mathfrak{S}_n$ に対して，

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$$

なる X の置換を考えると，$\sigma\sigma^{-1} = \sigma^{-1}\sigma = 1_{\mathfrak{S}_n}$ を満たす．したがって，以上のことから $\mathfrak{S}_n$ は写像の合成を積として群になることが分かる．この $\mathfrak{S}_n$ を n 次の**対称群** (symmetric group of degree n) という．$|\mathfrak{S}_n| = n!$ であるから，$\mathfrak{S}_n$ は有限群である．

$n = 1$ のとき，$\mathfrak{S}_1$ は恒等置換しか含まない．また，$n = 2$ のとき，$\mathfrak{S}_2$ は恒等置換と

$$\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

の二つの元しか含まない．よって，$n \leq 2$ のとき，$\mathfrak{S}_n$ はアーベル群である．以下，$n \geq 3$ のとき $\mathfrak{S}_n$ が非可換群であることを示そう．そこで，

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}$$

なる $\mathfrak{S}_n$ の二つの元を考える．このとき，

[18] すなわち，X 上の恒等写像のことである．

$$\sigma\tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\tau\sigma = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

であるから，$\sigma\tau \neq \tau\sigma$ である．よって，$n \geq 3$ のとき $\mathfrak{S}_n$ は非可換群である．

1.2.2 正二面体群

$n \geq 3$ を自然数とし，正 n 角形 V_n を考える．V_n を V_n 自身の上に合同に重ねあわせる操作を考える．これは，V_n から V_n への全単射であって，V_n 内の任意の二点間の距離を変えない写像になっている．このような写像を V_n の**合同変換** (congruent transformation) という．V_n の合同変換全体を

$$D_n := \{\sigma \mid \sigma \text{ は } V_n \text{ の合同変換 }\}$$

とおくと，D_n は写像の合成に関して群をなす．これを n 次の**正二面体群** (dihedral group) という．

D_n のすべての合同変換は，V_n の頂点たちの対応によって完全に決定される．実際，V_n の頂点に，時計回りの方向に順に $1, 2, \ldots, n$ と番号を付ける．V_n の合同変換 ρ に対して，ρ によって 1 が i に写されたとする．すると，残りの頂点 $2, 3, \ldots, n$ は ρ によって，それぞれ $i+1, i+2, \ldots, n, 1, 2, \ldots i-1$ に写されるか，$i-1, i-2, \ldots, 1, n, n-1, \ldots, i+1$ に写されるかのどちらかである．すなわち，ρ を置換の記法で表せば，

$$\rho = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i & i+1 & \cdots & i-2 & i-1 \end{pmatrix} \text{ または }$$

$$\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i & i-1 & \cdots & i+2 & i+1 \end{pmatrix}$$

となる．前者の場合は V_n を回転して重ねあわせる変換であり，後者の場合は V_n を回転してさらに裏返しして重ねあわせる変換である．したがって，V_n の合同変換は，頂点 1 をどの頂点に写すかで n 通り，さらに裏返しをするかしないかで 2 通りの場合があるから，

全部で $2n$ 個あることが分かる．すなわち，D_n は位数 $2n$ の有限群である．

$n=3$ とすると，$|D_3|=6$ である．具体的に元を（置換の記法で）書き下せば，D_3 は $\mathfrak{S}_3$ にほかならないことが分かる．

1.2.3　可換環上の一般線型群

この項では，前節に解説した K 上の 2 次の一般線型群 $\mathrm{GL}(2,K)$ に対して，係数および次数を拡張することを考える．以下，読者の方は線型代数および環論の初歩的な知識をある程度ご存知であるとして話を進める（初学者は読み飛ばしていただいてもまったく問題ない）．本節では，R を可換環とする．

$n \geq 1$ とし，R の元を成分とする n 次正方行列 A に対して，R の元を成分とするある n 次正方行列 B が存在して，

$$AB = BA = E_n \tag{1.3}$$

となるとき，A は**正則** (regular) であるという．ここで，E_n は n 次の単位行列を表す．A が正則であれば，(1.3) より，

$$1 = \det E_n = \det AB = (\det A)(\det B)$$

となる．A, B の各成分は R の元であるからそれらの行列式も R の元である．よって，A が正則であれば $\det A$ は R の単元であることが分かる．逆に，$\det A$ が単元となるような行列 P は正則である．実際，A の逆行列は以下のようにして求められる．$A=(a_{ij})$ とおくとき，その第 i 行と第 j 列を取り除いて得られる，$(n-1)$ 次の正方行列を $A_{\langle ij\rangle}$ と書く．すなわち，

$$A_{\langle ij\rangle} = \begin{pmatrix} a_{11} & \cdots & a_{1,j-1} & a_{1,j+1} & \cdots & a_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,j-1} & a_{i-1,j+1} & \cdots & a_{i-1,n} \\ a_{i+1,1} & \cdots & a_{i+1,j-1} & a_{i+1,j+1} & \cdots & a_{i+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{n,j-1} & a_{n,j+1} & \cdots & a_{nn} \end{pmatrix} \tag{1.4}$$

である．このとき，

$$A_{ij} = (-1)^{i+j} \det A_{\langle ij \rangle}$$

を A の (i,j) **余因子** (cofactor) といい，

$$\widetilde{A} = (A_{ji})$$

を A の**余因子行列** (adjugate matrix) [19] という．以上の記号の下，

$$A^{-1} = \frac{1}{\det A}\widetilde{A} \tag{1.5}$$

が成り立つ．このとき，$\det A$ が R の単元であれば，$\frac{1}{\det A}$ が R の元として意味を持つことに注意されたい．よって，

$$A \text{ が正則} \iff \det A \text{ が } R \text{ の単元}$$

を得る．

[19] (i,j) 成分が A の (i,j) 余因子 A_{ij} である行列も A の**余因子行列**ということがある．ただし，英語では cofactor matrix と書く．すなわち，adjugate matrix と cofactor matrix は転置の関係にある．

定義 1.10（可換環上の一般線型群） $n \geq 1$ に対して，R の元を成分とする n 次正則行列全体を $\mathrm{GL}(n,R)$ とおく．すると，通常の行列の積に関して $\mathrm{GL}(n,R)$ は群になる．実際，行列の積が結合法則を満たすことが知られており，単位元および，任意の行列 $A \in \mathrm{GL}(n,R)$ の逆元はそれぞれ，単位行列 E_n および，A の逆行列 A^{-1} である．そこで，この $\mathrm{GL}(n,R)$ を R 上の n 次の**一般線型群** (general linear group) という．

上で述べたことより，

$$\mathrm{GL}(n,R) = \{A \mid A \text{ は } n \text{ 次正方行列で } \det A \text{ は } R \text{ の単元}\}$$

となる．

特に，$R = \mathbb{Z}$ のとき，$\mathbb{Z}$ の単元は ± 1 であるから

$$\mathrm{GL}(n,\mathbb{Z}) = \{P \mid P \text{ は } n \text{ 次正方行列で } \det P = \pm 1\}$$

である．

1.3 問題

問題 1.1 以下の集合 G, および G 上の演算に関して G は群をなさない. その理由を述べよ.

(1) $G = \mathbb{N}$ で, 演算は自然数の通常の加法.
(2) $G = \mathbb{Z}$ で, 演算は整数の通常の乗法.
(3) $G = \mathbb{Q}$ で, 演算は有理数の通常の乗法.

解答. (1) 単位元が存在しない. (2) 任意の $n \geq 2$ に対して, $\pm n$ の逆元が存在しない. (3) 0 の逆元が存在しない. □

問題 1.2 0 でない任意の実数 a と, 任意の実数 b に対して, 写像 $\sigma_{a,b} : \mathbb{R} \to \mathbb{R}$ を

$$x \mapsto ax + b$$

で定める.

(1) 各 $\sigma_{a,b}$ は全単射であることを示せ.
(2) $G := \{\sigma_{a,b} \mid a \in \mathbb{R} \setminus \{0\},\ b \in \mathbb{R}\}$ とおくとき, G は写像の合成に関して群をなすことを示せ.

解答. (1) $\sigma_{a^{-1},-a^{-1}b}$ が $\sigma_{a,b}$ の逆写像である. よって, $\sigma_{a,b}$ は全単射.
(2) 任意の $a, a' \in \mathbb{R} \setminus \{0\}$, $b, b' \in \mathbb{R}$ および, 任意の $x \in \mathbb{R}$ に対して,

$$\begin{aligned}\sigma_{a,b} \circ \sigma_{a',b'}(x) &= \sigma_{a,b}(a'x + b') = aa'x + ab' + b \\ &= \sigma_{aa',ab'+b}(x)\end{aligned}$$

であるから, G は積に関して閉じている. また結合法則が成り立つことは写像の合成から明らか. 単位元は $\sigma_{1,0} = \mathrm{id}_{\mathbb{R}}$ であり, $\sigma_{a,b}$ の逆元は $\sigma_{a^{-1},-a^{-1}b}$ である. よって, G は群である. □

問題 1.3 G を位数が 4 以下の群とするとき, G はアーベル群であることを示せ.

解答. $|G|=1$ のときは $G=\{1_G\}$ ゆえ明らか. $|G|=2$ のとき, $G=\{1_G,a\}$ なる形をしている. 一般に, 単位元は任意の元と可換ゆえ, G はアーベル群となる.

$|G|=3$ のとき. $G=\{1_G,a,b\}$ と書ける. $ab=ba$ なることを示せばよい. 特に, $ab=1_G$ である. 実際, $ab=a$ とすると, 両辺に左から a^{-1} を乗じて $b=1_G$ となるので矛盾. 同様に, $ab=b$ とすると $a=1_G$ となり矛盾. よって, $ab=1_G$ である. 同様に $ba=1_G$ であることも示される. よって, $ab=ba$ となり, G はアーベル群である.

$|G|=4$ のとき. $G=\{1_G,a,b,c\}$ と書ける. $ab=ba$, $ac=ca$, $bc=cb$ を示せばよい. 対称性から $ab=ba$ のみ示せば十分である. まず, 上と同様の議論により, $ab\neq a,b$ である. $ab=1_G$ のときは, 両辺に左から b, 右から b^{-1} を乗じて, $ba=1_G$ となり, $ab=ba$ を得る. そこで, $ab=c$ とする. 同様の議論により, $ba=1_G$ または c である. もし, $ba=1_G$ とすると $ab=1_G$ であり, $c=1_G$ となって矛盾. よって, $ba=c$ でなければならない. すなわち, $ab=ba$ である. 他の場合も同様にして示される. □

問題 1.4 乗法群 G において, 任意の元 $x\in G$ に対し $x^2=1_G$ が成り立つならば, G はアーベル群であることを示せ.

解答. まず, 任意の $x\in G$ に対して, $x^{-1}=x$ であることに注意する. このとき, 任意の $x,y\in G$ に対して,

$$xy=(xy)^{-1}=y^{-1}x^{-1}=yx$$

となるので, G はアーベル群である. □

問題 1.5 自然数 $n\geq 3$ に対して, n 次対称群 $\mathfrak{S}_n$ を考える. 各 $1\leq i\leq n-1$ に対して,

$$\sigma_i:=\begin{pmatrix} i & i+1 \\ i+1 & i \end{pmatrix}$$

とおく. このとき, 以下の等式が成り立つことを確かめよ.

(1)$\sigma_i\sigma_{i+1}\sigma_i=\sigma_{i+1}\sigma_i\sigma_{i+1}$ $(1\leq i\leq n-2)$

(2)$\sigma_i\sigma_j = \sigma_j\sigma_i$ $(|i-j| \geq 2)$
(3)$\sigma_i^2 = 1$ $(1 \leq i \leq n-1)$

解答. 直接確かめればよい. □

問題 1.6 $n \geq 2$ を自然数，R を可換環とする.

(1) $\mathrm{GL}(n, R)$ は非可換群であることを示せ.
(2) R が無限集合のとき，$\mathrm{GL}(n, R)$ は無限群であることを示せ.

解答. (1) 例えば，$n = 2$ のとき，$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(n, R)$ とおくと，

$$AB = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \quad BA = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$$

であるから求める結果を得る. $n \geq 3$ の場合は，$\begin{pmatrix} A & O \\ O & E_{n-2} \end{pmatrix}$, $\begin{pmatrix} B & O \\ O & E_{n-2} \end{pmatrix}$ を考えればよい.

(2) 例えば，任意の $a \in R$ に対して，$\begin{pmatrix} E_{n-2} & O & O \\ O & 1 & a \\ O & 0 & 1 \end{pmatrix}$ なる行列たちを考えればよい. □

問題 1.7 整数を成分とする 3 次正方行列

$$\begin{pmatrix} 1 & 2 & 3 \\ -2 & 0 & 1 \\ -1 & 2 & 4 \end{pmatrix}, \quad \begin{pmatrix} 0 & -2 & 1 \\ -5 & 0 & 1 \\ 2 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & -1 \end{pmatrix}$$

を考える.

(1) $\mathrm{GL}(3, \mathbb{Q})$ の元であるものをすべて選べ.
(2) $\mathrm{GL}(3, \mathbb{Z})$ の元であるものをすべて選べ.

解答. 行列式を計算すればよい.

(1) $\begin{pmatrix} 0 & -2 & 1 \\ -5 & 0 & 1 \\ 2 & 1 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & -1 \end{pmatrix}$.

(2) $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & -1 \end{pmatrix}$. □

2 部分群とその性質

一般に，群を与えるとその部分集合でまた群になっているようなものがある．このようなものを部分群という．ガロア理論におけるガロア対応など，与えられた群がどのような部分群をどの程度有するかを調べることは応用上重要である．本章では部分群に関するいくつかの性質を解説する．

2.1 部分群

定義 2.1（**部分群**）群 G の空でない部分集合 $H \subset G$ が，

(1) 任意の $x, y \in H$ に対して，$xy \in H$,
(2) 任意の $x \in H$ に対して，$x^{-1} \in H$

を満たすとき，H は G の積を H に制限することによって群になることが分かる．実際，H は二つの元の積を取る操作，および各元の逆元を取る操作で閉じており，積に関して結合法則が成り立つことは既に G において成立していることから明らか．また，H は空でないのである $x \in H$ が存在する．すると (2) から $x^{-1} \in H$ であり，(1) より $1_G = xx^{-1} \in H$ となる．この 1_G が H の単位元になる．このような H を G の**部分群** (subgroup) という．H が G の部分群であるとき，$H \leq G$ と表す．もちろん，$G \leq G$ である．

定義から分かるように，部分群の単位元はもとの群の単位元と一致する．すなわち，$1_H = 1_G$ である．$\{1_G\}$ を G の**自明な部分群** (trivial subgroup) という．G の部分群で G とも $\{1_G\}$ とも異なるものを G の**真部分群** (proper subgroup) という．

例 2.2 (1) 加法群 $\mathbb{Z}$ において，自然数 $n \geq 1$ の倍数全体のなす部分集合

$$n\mathbb{Z} := \{0, \pm n, \pm 2n, \ldots\} \subset \mathbb{Z}$$

を考える．すると，$0 \in n\mathbb{Z}$ である．また，任意の $x, y \in n\mathbb{Z}$ に対して，$x = nk, y = nl$ なる整数 $k, l \in \mathbb{Z}$ が存在し，

$$x + y = n(k + l), \quad -x = n(-k) \in n\mathbb{Z}$$

となるので，$n\mathbb{Z}$ は $\mathbb{Z}$ の加法部分群である．

(2) 前章でも述べたとおり，自然数 $n \geq 1$ に対して，正二面体群 D_n は対称群 $\mathfrak{S}_n$ の部分群とみなせる．

補題 2.3 G を群，H, K を G の部分群とする．このとき，$H \cap K$ は G の部分群である．

証明． まず，$1_G \in H \cap K$ であるから $H \cap K \neq \emptyset$．次に，任意の $x, y \in H \cap K$ とする．$x, y \in H$ であり，H は部分群であるので $xy \in H$．同様にして，$xy \in K$．よって，$xy \in H \cap K$．一方，任意の $x \in H \cap K$ に対して，$x^{-1} \in H \cap K$ となることも同様の議論から分かる．よって，$H \cap K$ は G の部分群である．□

次に，群 G とその部分集合 S が与えられたときに，S を用いて G の部分群を構成することを考えよう．一般に，任意の $g \in G$ に対して

$$gS := \{gs \in G \,|\, s \in S\} \subset G$$
$$Sg := \{sg \in G \,|\, s \in S\} \subset G$$

と定義する．つまり，gS は S の各元に左から g を掛けて得られるような G の元全体の集合である．Sg についても同様である．

補題 2.4 群 G と任意の元 $g \in G$ に対して，$gG = G = Gg$ である．

証明． $gG = G$ を示す．$Gg = G$ についても同様である．$gG \subset G$ は明らかゆえ，$G \subset gG$ を示せばよい．すると，任意の $x \in G$ に対して，

$$x = (gg^{-1})x = g(g^{-1}x) \in gG$$

となるので，直ちに $G \subset gG$ が得られる．□

定義 2.5（**正規化群**）群 G とその部分集合 $S \subset G$ に対して，

$$N_G(S) := \{g \in G \mid gS = Sg\}$$

とおくと，$N_G(S)$ は G の部分群になる．実際，$1_G \in N_G(S)$ であるから $N_G(S) \neq \emptyset$．また，任意の $g, h \in N_G(S)$ に対して，結合法則を用いて

$$\begin{aligned}(gh)S &= \{(gh)s \mid s \in S\} = \{g(hs) \mid s \in S\} = g(hS) = g(Sh)\\ &= \{g(sh) \mid s \in S\} = \{(gs)h \mid s \in S\} = (gS)h = (Sg)h\\ &= \{(sg)h \mid s \in S\} = \{s(gh) \mid s \in S\} = S(gh)\end{aligned}$$

となるので，$gh \in N_G(S)$．さらに，任意の $g \in N_G(S)$ に対して，

$$\begin{aligned}g^{-1}S &= \{g^{-1}s \mid s \in S\} = \{(g^{-1}s)(gg^{-1}) \mid s \in S\}\\ &= \{(g^{-1}(sg))g^{-1} \mid s \in S\}\\ &= (g^{-1}(Sg))g^{-1} = (g^{-1}(gS))g^{-1} = Sg^{-1}\end{aligned}$$

となるので，$g^{-1} \in N_G(S)$ である．よって，$N_G(S)$ は G の部分群である．$N_G(S)$ を G における S の**正規化群** (normalizer) という．

定義 2.6（**中心化群，中心**）群 G とその部分集合 $S \subset G$ に対して，

$$C_G(S) := \{g \in G \mid \text{任意の } s \in S \text{ に対して } gs = sg\}$$

とおくと，$C_G(S)$ は G の部分群になる．実際，$1_G \in C_G(S)$ であるから $C_G(S) \neq \emptyset$．また，任意の $g, h \in C_G(S)$ と任意の $s \in S$ に対して，

$$(gh)s = g(hs) = g(sh) = (gs)h = (sg)h = s(gh)$$

となるので，$gh \in C_G(S)$．さらに，任意の $g \in C_G(S)$ と任意の $s \in S$ に対して，

$$g^{-1}s = (g^{-1}s)(gg^{-1}) = (g^{-1}(sg))g^{-1} = (g^{-1}(gs))g^{-1} = sg^{-1}$$

となるので，$g^{-1} \in C_G(S)$ である．よって，$C_G(S)$ は G の部分群

である．$C_G(S)$ を G における S の**中心化群** (centralizer) という．特に，G における G 自身の中心化群 $C_G(G)$ を G の**中心** (center) といい，$Z(G)$ と書く．

$N_G(S)$ および $C_G(S)$ が部分群であることを確かめる際に，結合法則が重要な役割を果たしていることがご理解いただけたのではないかと思う．

さて，正規化群と中心化群はどちらも似たような定義であるが，中心化群の定義に現れる条件のほうが，正規化群のそれよりも厳しい．いい換えれば，次のことが成り立つ．

命題 2.7 群 G とその部分集合 $S \subset G$ に対して，$C_G(S) \leq N_G(S)$.

証明. 両者はともに G の部分群であることは分かっているので，$C_G(S) \subset N_G(S)$ を示せばよい．任意の $g \in C_G(S)$ をとる．このとき，任意の $s \in S$ に対して $gs = sg$ が成り立つから，

$$gS = \{gs \in G \mid s \in S\} = \{sg \in G \mid s \in S\} = Sg$$

となり，$g \in N_G(S)$ であることが分かる．よって，$C_G(S) \subset N_G(S)$.
□

G がアーベル群のときは，定義から分かるように $C_G(S) = N_G(S) = G$ である．一般に，G が非可換群のとき，$C_G(S)$ と $N_G(S)$ は異なる．簡単な例を一つ挙げておこう．3 次対称群

$$\mathfrak{S}_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

において，

$$S := \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} \subset \mathfrak{S}_3$$

なる部分集合を考える．このとき，簡単な計算によって，$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ のとき，

$$\sigma\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\sigma,\quad \sigma\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\sigma$$

であり，$\tau=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ のとき，

$$\tau\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\tau,\quad \tau\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\tau$$

であることが分かるので，

$$C_{\mathfrak{S}_3}(S)=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\},$$
$$N_{\mathfrak{S}_3}(S)=\mathfrak{S}_3$$

となる．

命題 2.8 G を群とし，H を G の部分群とする．このとき，$H \leq N_G(H)$ である．

証明. H と $N_G(H)$ はともに G の部分群であるから，$H \subset N_G(H)$ であることを示せばよい．そこで，任意の $h \in H$ をとる．このとき，補題 2.4 によって，$hH = H = Hh$ であるから，明らかに $h \in N_G(H)$ となる．□

次に，群 G とその部分集合 S が与えられたときに，S を含むような部分群の中で"一番小さい" [20] ものはどのようなものかについて考える．

[20] 自然な包含関係によって G の部分集合たちの間に順序関係を入れるとき，その順序によって最小元という意味である．

定義 2.9（生成された部分群） 群 G と部分集合 $S \subset G$ に対して，S の元，もしくは S の元の逆元の有限個の積として表せる G の元全体を

$$\langle S\rangle := \{s_1^{e_1}s_2^{e_2}\cdots s_m^{e_m} \mid m\in\mathbb{Z}_{\geq 0},\ s_i\in S,\ e_i=\pm 1\}$$

とおく．特に，1_G は 0 個の S の元による積とみなし，$1_G \in \langle S\rangle$ と考える．すると，$\langle S\rangle$ は G の部分群になる．実際，$1_G \in \langle S\rangle$ であるから $\langle S\rangle \neq \emptyset$ であり，任意の $\sigma = s_1^{e_1}s_2^{e_2}\cdots s_m^{e_m}$, $\tau = t_1^{f_1}t_2^{f_2}\cdots t_n^{f_n}$

$\in \langle S \rangle$ $(s_i, t_j \in S)$ に対して，

$$\sigma\tau = s_1^{e_1} s_2^{e_2} \cdots s_m^{e_m} t_1^{f_1} t_2^{f_2} \cdots t_n^{f_n} \in \langle S \rangle$$

であるから，$\langle S \rangle$ は積について閉じている．また，任意の $\sigma = s_1^{e_1} s_2^{e_2} \cdots s_m^{e_m} \in \langle S \rangle$ に対して，$\sigma^{-1} = s_m^{-e_m} s_{m-1}^{-e_{m-1}} \cdots s_1^{-e_1} \in \langle S \rangle$ が σ の逆元である．

$\langle S \rangle$ を S **によって生成された部分群** (subgroup generated by S) という．特に，$G = \langle S \rangle$ となるとき，S を G の**生成系** (generating system) といい，S の元を G の**生成元** (generator) という．また，S が有限集合のとき G を**有限生成群** (finitely generated group) といい，有限生成でない群を**無限生成群** (infinitely generate group) という[21]．

[21] 無限生成群とは，有限部分集合をどのようにとってもそれで生成されないような群のことであり，無限個の元で生成されている群を指すわけではない．例えば，加法群 $\mathbb{Z}$ は $\mathbb{Z}$ 自身を生成系とみなせば無限個の元で生成されるが，$\{1\}$ が生成系であるので有限生成群である．

任意の有限群 G は（極端ではあるが）G 自身を生成系とみなすことができるので有限生成群である．一般に，与えられた群に対してどれだけ便利な生成系を構成できるかということはしばしば重要な問題であるが，一概に数が少ないほどよいかというと，そういうわけでもない．場合によっては元の個数は多くても対称性が高くて扱いやすい生成系が求められることもある．

命題 2.10 G を群, $S \subset G$ を G の部分集合とする．このとき, $S \subset H$ なる G の任意の部分群 H に対して，$\langle S \rangle \leq H$．すなわち，$\langle S \rangle$ は S を含むような G の部分群の中で最小の部分群である．

証明. $\langle S \rangle$ も H も G の部分群であるので，$\langle S \rangle \subset H$ となることを示す．そこで，任意の $\sigma \in \langle S \rangle$ とすると，$\sigma = s_1^{e_1} s_2^{e_2} \cdots s_m^{e_m}$ $(s_i \in S,\ e_i = \pm 1)$ とかける．このとき，仮定より，各 $1 \leq i \leq m$ に対して，$s_i \in H$ である．H は群であり，積をとる操作と逆元をとる操作で閉じているので，$\sigma \in H$ である．よって，$\langle S \rangle \leq H$ となる．□

例 2.11 自然数 $n \geq 1$ に対して，1 の複素 n 乗根全体のなす群 $\mathcal{U}_n$ を考える．任意の $0 \leq k \leq n-1$ に対して，

$$\exp\Bigl(\frac{2k\pi\sqrt{-1}}{n}\Bigr) = \exp\Bigl(\frac{2\pi\sqrt{-1}}{n}\Bigr)^k$$

であるから，$\mathcal{U}_n = \langle \exp\left(\frac{2\pi\sqrt{-1}}{n}\right) \rangle$ である．

例 2.12 自然数 $n \geq 3$ に対して，n 次の正二面体群 D_n を考える．σ を，V_n を時計回りに $\frac{2\pi}{n}$ 回転させる合同変換とし，τ を頂点 1 を固定する裏返しを表す合同変換

$$\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 1 & n & \cdots & 3 & 2 \end{pmatrix}$$

とすると，$D_n = \langle \sigma, \tau \rangle$ である．実際，V_n の頂点 i を固定する裏返しを表す合同変換を τ_i とすると，

$$D_n := \{\sigma^{i-1}, \tau_i\sigma^{i-1} \,|\, 1 \leq i \leq n\}$$

である．一方，任意の $1 \leq i \leq n-1$ に対して，$\tau_i = \sigma^{i-1}\tau\sigma^{-(i-1)}$ であるから，結局，D_n は σ と τ で生成されることが分かる．特に，

$$D_n = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \ldots, \sigma^{n-1}\tau\}$$

である．また，明らかに $\sigma^n = \tau^2 = 1_{D_n}$ であり，

$$\begin{aligned} \tau\sigma &= \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 1 & n & \cdots & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix} \\ \sigma^{-1}\tau &= \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & 1 & \cdots & n-2 & n-1 \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 1 & n & \cdots & 3 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix} \end{aligned}$$

となるので，$\tau\sigma = \sigma^{-1}\tau$ が成り立つ．

群 G とその部分集合 $S, T \subset G$ に対して，

$$ST := \{st \in G \,|\, s \in S,\ t \in T\}$$

と定める．

定義 2.13（**左剰余類**）G の部分群 H，および $g \in G$ に対して gH なる形の G の部分集合を G における H の**左剰余類** (left coset) と

いう．H の**右剰余類** (right coset) Hg についても同様に定義されるが，本書では特に断らない限り使用しない．以下，左剰余類を単に剰余類と略記する．

G における H の相異なる剰余類の個数（無限の場合もありうる）を，G における H の**指数** (index) といい，$[G:H]$ と表す．

命題 2.14 G を群，H を部分群とする．

(1) 各 $x \in G$ に対して，x を含む H の剰余類がただ一つ存在し，それは xH である．

(2) $x, y \in G$ に対して，

$$xH = yH \quad \text{または} \quad xH \cap yH = \emptyset$$

が成り立つ．

(3) G は互いに交わらないような剰余類の和集合として表すことができる．

証明． (1) $1 \in H$ であるから，$x = x \cdot 1 \in xH$ である．一方，$x \in yH$ とすると，$yH = xH$ となる．実際，$x \in yH$ とすると，ある元 $h_0 \in H$ で $x = yh_0$ となるものが存在する．このとき，任意の $h \in H$ に対して，$yh = (xh_0^{-1})h = x(h_0^{-1}h) \in xH$ となるので，$yH \subset xH$．逆に，任意の $h \in H$ に対して $xh = y(h_0h) \in yH$ でもあるので，$xH \subset yH$．ゆえに，$yH = xH$．つまり，x を含む H の剰余類はただ一つ xH のみである．

(2) $x, y \in G$ とし，$xH \neq yH$ と仮定する．このとき，$xH \cap yH = \emptyset$ であることを示せばよい．そこで，$xH \cap yH \neq \emptyset$ であると仮定すると，ある $z \in xH \cap yH$ が存在する．すると，ある $h_1, h_2 \in H$ であって，$z = xh_1$, $z = yh_2$ となるものがとれる．このとき，任意の $h \in H$ に対して，

$$xh = (zh_1^{-1})h = z(h_1^{-1}h) = (yh_2)(h_1^{-1}h) = y(h_2h_1^{-1}h) \in yH$$

となるので，$xH \subset yH$．まったく同様にして $yH \subset xH$ を得る．よって，$xH = yH$ となり，これは仮定に矛盾である．よって，$xH \cap yH = \emptyset$.

(3) まず,

$$G = \bigcup_{x \in G} xH$$

に注意する．実際，$\supset$ の包含関係は明らかである．(1) より，任意の $y \in G$ に対して $y \in yH$ であるから $y \in \bigcup_{x \in G} xH$ となり，$\subset$ の包含関係も分かる．

次に，(2) より，G の H による剰余類たちは，ぴったり一致するか共通部分をまったく持たないかのどちらかしかないので，$\bigcup_{x \in G} xH$ において重複があるものをすべて取り除けば，互いに交わらないような剰余類の和集合として G を表すことができる．□

上の命題の (3) によって得られる，互いに交わらないような G の H による剰余類たちの和集合による表示を，G の H による**剰余類分割** (coset decomposition) という．

注意 2.15 G を群，H を部分群とする．$x, y \in G$ に対して，$x^{-1}y \in H$ となるとき，

$$x \equiv y \pmod{H}$$

と書くことがある．これは G 上の同値関係である．実際，

(1) 任意の $x \in G$ に対して，$x^{-1}x = 1 \in H$ であるから，$x \equiv x \pmod{H}$.

(2) $x, y \in G$ に対して，$x \equiv y \pmod{H}$ とすると，$x^{-1}y \in H$．すると，H は群であるから，

$$(x^{-1}y)^{-1} = y^{-1}x \in H$$

となる．よって，$y \equiv x \pmod{H}$.

(3) $x, y, z \in G$ に対して，$x \equiv y \pmod{H}$ かつ，$y \equiv z \pmod{H}$ とすると，$x^{-1}y, y^{-1}z \in H$ であるから，

$$(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$$

となり，$x \equiv z \pmod{H}$.

である．このとき，剰余類 xH は，この同値関係における x の属する同値類にほかならない．一般に，

$$x \equiv y \pmod H \iff \text{ある } h \in H \text{ が存在して } y = xh \text{ となる.}$$
$$\iff xH = yH$$

である.

定理 2.16（ラグランジュの定理） G を群，$H \subset G$ を部分群とする．このとき，$|G| = |H|\,[G:H]$ が成り立つ[22]．特に，G が有限群であれば，G の部分群の位数は G の位数の約数である.

22) G と H のいずれかがが無限群の場合であっても，$\infty = \infty$ という意味で与式は成り立つが，もちろん応用上重要なのは G が有限群のときである.

証明. G の H による各剰余類がすべて，H と同じ個数の要素を含むことを示せばよい．そこで，任意の $g \in H$ に対して，$|gH| = |H|$ となることを示そう．写像 $f : H \to gH$ を各 $h \in H$ に対して，$f(h) := gh$ によって定めるとき，f が全単射であることを示す.

まず, $x, y \in H$ に対して, $f(x) = f(y)$ となったとすると, $gx = gy$ となる. この式の両辺に左から g^{-1} を乗じれば，$x = y$ を得る．したがって，f は単射である．次に，任意の $z \in gH$ に対して，ある $h \in H$ が存在して $z = gh$ と書ける．このとき，$f(h) = z$ である．すなわち，f は全単射である．これより求める結果を得る．□

注意 2.17 G を有限群とするとき，一般に，ラグランジュの定理の逆は成り立たない．例 4.18 参照.

2.2 正規部分群と剰余群

この節では，群上である種の同値関係を考え，その同値類たちの集合（商集合）に“自然な”群の構造を入れることを考える.

群 G と部分集合 $S \subset G$ を考える．各 $g \in G$ に対して,

$$gSg^{-1} := \{gsg^{-1} \mid s \in S\}$$

とおく.

定義 2.18（正規部分群） 群 G の部分群 $N \subset G$ が，任意の $g \in G$ に対して，$gNg^{-1} \subset N$ を満たすとき，N を G の**正規部分群** (normal subgroup) という．このとき，$N \lhd G$ と書く.

補題 2.19 G を群とするとき，以下が成り立つ．

$$
\begin{aligned}
N \text{ が } G \text{ の正規部分群} &\iff \text{任意の } g \in G,\, n \in N \text{ に対して} \\
&\qquad gng^{-1} \in N \\
&\iff \text{任意の } g \in G \text{ に対して } gNg^{-1} = N \\
&\iff \text{任意の } g \in G \text{ に対して } gN = Ng
\end{aligned}
$$

証明. 最初の $(\Leftrightarrow)$ は定義そのものである．二番目の $(\Leftrightarrow)$ については，N が G の正規部分群のとき，任意の $g \in G$ に対して $N \subset gNg^{-1}$ となることを示せばよい．そこで，任意の $n \in N$ に対して，N は正規部分群であるから $g^{-1}ng \in N$ である．よって，$g^{-1}ng = m$, $m \in N$ と書けるのでこれを用いると，$n = gmg^{-1} \in N$ であることが分かる．すなわち，$N \subset gNg^{-1}$ を得る．三番目の $(\Leftrightarrow)$ については以下のようになる．N を G の正規部分群とする．任意の $g \in G$ と $n \in N$ に対して，$gNg^{-1} = N$ を用いると，$gng^{-1} = m \in N$ なる $m \in N$ がとれる．このとき，$gn = mg$．つまり，$gN \subset Ng$ となる．また，$g^{-1}Ng = N$ より，$g^{-1}ng = m' \in N$ となる $m' \in N$ がとれる．このとき，$ng = gm'$ となり，$gN \supset Ng$ を得る．したがって，$gN = Ng$ である．

逆に，任意の $g \in G$ に対して $gN = Ng$ であるとする．このとき，任意の $n \in N$ に対してある $m \in N$ が存在して $gn = mg$ となるので，$gng^{-1} = m \in N$ を得る．すなわち，$gNg^{-1} \subset N$ となり，N は G の正規部分群である．□

注意 2.20 上の補題の三つ目の条件から，$N \lhd G$ のとき，N の G における正規化群 $N_G(N)$ は G そのものであることが分かる．また，任意の部分群 $H \leq G$ に対して，命題 2.8 より $H \leq N_G(H)$ であったが，上の三つ目の条件を考慮すれば，$H \lhd N_G(H)$ であることが分かる．

命題 2.21 G をアーベル群とする．このとき，G の任意の部分群は正規部分群である．すなわち，アーベル群 G においては，部分群と正規部分群の区別はない．

証明. H を G の部分群とする．任意の $g \in G$ および任意の $h \in H$

に対して，$ghg^{-1} = h$ であるから，$gHg^{-1} = H$．よって，$H \lhd G$ である．□

例 2.22 3 次対称群 $\mathfrak{S}_3$ において，

$$N := \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} \subset \mathfrak{S}_3$$

なる部分集合を考える．すると，

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

となるから，N は $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ が生成する $\mathfrak{S}_3$ の部分群であることが分かる．さらに，

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$\begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

より，N は $\mathfrak{S}_3$ の正規部分群であることが分かる．

補題 2.23 G を群，K を G の部分群，N を G の正規部分群とする．このとき，KN は G の部分群である．

証明. まず，$1_G \in K \cap N$ であり，$1_G = 1_G \cdot 1_G \in KN$ であるので，$KN \neq \emptyset$．次に，任意の $x, y \in KN$ に対して，$x = k_1 n_1$，$y = k_2 n_2$，$k_1, k_2 \in K$，$n_1, n_2 \in N$ とすれば，

$$xy = k_1 n_1 k_2 n_2 = k_1 k_2 (k_2^{-1} n_1 k_2) n_2,$$
$$x^{-1} = n_1^{-1} k_1^{-1} = k_1^{-1} (k_1 n_1^{-1} k_1^{-1})$$

であるから，N が G の正規部分群であることに注意すれば，$xy, x^{-1} \in KN$ となることが分かる．ゆえに，KN は G の部分群である．□

注意 2.24 一般に，群 G の部分群 H, K に対して，HK は G の部分群にはならない．実際，$\mathfrak{S}_3$ において，

$$H := \left\{ 1_{\mathfrak{S}_3}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}, \quad K := \left\{ 1_{\mathfrak{S}_3}, \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix} \right\}$$

を考えると，HK は位数 4 の部分集合となるが，ラグランジュの定理より，これは $\mathfrak{S}_3$ の部分群とはならない．

定義 2.25（剰余群） 群 G とその正規部分群 N に対して，剰余類の集合 $G/N := \{gN \mid g \in G\}$ には以下のようにして自然に群の構造が入る．

G/N の二つの元 xN, yN に対して，その積を

$$xN \cdot yN := (xy)N$$

によって定める．これは各剰余類の代表元のとり方によらない．実際，$xN = x'N, yN = y'N$ と仮定すると，ある $m, m' \in N$ が存在して，$x' = xm, y' = ym'$ と書ける．このとき，

$$x'y' = xmym' = xy \cdot (y^{-1}my)m'$$

となる．ここで，$y^{-1}mym' \in N$ に注意すれば，補題 2.4 を用いて

$$\begin{aligned} (x'y')N &= \{(x'y')n \mid n \in N\} = \{(xy)(y^{-1}mym')n \mid n \in N\} \\ &= (xy)((y^{-1}mym')N) = (xy)N \end{aligned}$$

を得る．

なぜこのような議論が必要なのかというと，xN および，yN はあくまで見かけ上の “仮の姿” であって，$x' \in xN$，$y' \in yN$ なる元を持ってくれば，$xN = x'N$，$yN = y'N$ となって簡単に姿が化けてしまう．一般に，群の元 σ，τ に対して，それらの積 $\sigma \cdot \tau$ は一意的に定まっていないといけない．したがって，今の場合も xN および，yN が別の姿になったときにその積が “ぶれずに” 一意的であることをきちんと確かめなければならない．そのための議論である．専門的ないい方をすれば，上で定義した積が，剰余類の代表元の取り方によらず well-defined [23] であることを確かめるのである．

さて，この積に関して結合法則が成り立つのは，G の積が結合法則

[23] 整合性がとれて矛盾なく定義されている，という意味である．数学ではよく用いられる表現である．

を満たすことから明らかである．また，単位元は $1_G N = N$ であり，任意の gN に対して gN の逆元 $(gN)^{-1}$ は $g^{-1}N$ である．このようにして得られる群 G/N を G の N による**剰余群** (quotient group) という．

剰余群 G/N において，各元である剰余類 gN は $g \pmod N$ と表されることもある．また，前後の文脈から N が明らかに分かるときはそれを省略して，$[g]$ や $\overline{g}$ などと書かれることもある．さらに，もっと極端な場合，（記号の濫用であることは否めないが）同じ g で表されることもある[24)]．

[24)] 他の文脈との関係上，記号が過度に煩雑になるのを防ぐためであるが，このような極端な用法はプロ向けの研究論文などによく見られる．

例 2.26 剰余群の例で最も重要なもののうちの一つは，加法群 $\mathbb{Z}$ の剰余群であろう．自然数 $n \geq 1$ に対して，$n\mathbb{Z}$ は $\mathbb{Z}$ の部分群であった．特に，$\mathbb{Z}$ はアーベル群であるから，$n\mathbb{Z}$ は $\mathbb{Z}$ の正規部分群である．したがって，剰余群 $\mathbb{Z}/n\mathbb{Z}$ が定義される．

$\mathbb{Z}/n\mathbb{Z}$ は集合としては，$\mathbb{Z}$ における同値関係

$$x \sim y \iff n|(x-y)$$

による商集合にほかならない．よって，$\{0, 1, \dots, n-1\}$ は一つの完全代表系である．したがって，整数 $m \in \mathbb{Z}$ の属する剰余類を $[m]_n$ で表すことにすれば，

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \dots, [n-1]_n\}$$

となり，$\mathbb{Z}/n\mathbb{Z}$ は位数 n の有限アーベル群であることが分かる．特に，任意の整数 $a, b \in \mathbb{Z}$ に対して，

$$[a]_n + [b]_n = [a+b]_n, \quad -[a]_n = [-a]_n$$

である．

2.3 巡回群

この節では，巡回群に関する性質を詳しく解説する．特に，巡回群の生成元の形や個数，および部分群の個数を完全に決定する．本

節を読み進める前に，初等整数論に関する事項（巻頭にある記号の注意，および付録など）に目を通しておくことを推奨する．

定義 2.27（**巡回群**）G を群とする．ある $g \in G$ が存在して，$G = \langle g \rangle$ となるとき，G を**巡回群** (cyclic group) という．すなわち，一つの元で生成される群が巡回群である．巡回群 G は，有限群か無限群かによってそれぞれ，**有限巡回群** (finite cyclic group)，**無限巡回群** (infinite cyclic group) という．

例 2.28 自然数 $n \geq 1$ に対して，1 の複素 n 乗根全体のなす乗法群 $\mathcal{U}_n = \langle \exp\left(\frac{2\pi\sqrt{-1}}{n}\right) \rangle$ は位数 n の有限巡回群である．また，加法群 $\mathbb{Z} = \langle 1 \rangle$ は無限巡回群であり，その剰余群 $\mathbb{Z}/n\mathbb{Z} = \langle [1]_n \rangle$ は位数 n の有限巡回群である．

命題 2.29 G を巡回群とする．このとき，以下が成り立つ．

(1) G はアーベル群．
(2) G の任意の部分群，および剰余群は巡回群である．

証明．以下，$G = \langle g \rangle$ とする．

(1) 任意の $x, y \in G$ に対して，ある $m, n \in \mathbb{Z}$ が存在して $x = g^m$，$y = g^n$ となる．このとき，

$$xy = g^m g^n = g^{m+n} = g^n g^m = yx$$

となるので，G はアーベル群である．

(2) $H \leq G$ とする．$H = \{1_G\}$ の場合は明らかゆえ，$H \neq \{1_G\}$ とする．このとき，ある $g^m \in H$ $(m \neq 0)$ が存在する．もし $m < 0$ であれば，逆元を考えることにより，$(g^{-1})^{-m} \in H$ となるので，H には g^m $(m > 0)$ なる形の元が少なくとも一つは存在することが分かる．

そこで，

$$n := \min\{m \in \mathbb{N} \mid g^m \in H\}$$

とおく．すなわち，n は，$g^m \in H$ となるような $m > 0$ の中で最小のものである．このとき，$H = \langle g^n \rangle$ であることを示そう．$\supset$ は明らかゆえ，$\subset$ を示す．そのために，任意の $h \in H$ をとる．すると，

ある $l \in \mathbb{Z}$ が存在して，$h = g^l$ と書ける．このとき，剰余の定理を考えると

$$l = nq + r, \quad 0 \leq r < n$$

なる $q, r \in \mathbb{Z}$ がとれる．ここで，もし $r \neq 0$ とすると，$g^r = g^{l-nq} = g^l \cdot (g^n)^{-q} \in H$ となるが，これは n の最小性に矛盾である．したがって，$r = 0$ でなければならない．よって，$h = g^l = g^{nq} = (g^n)^q \in \langle g^n \rangle$ を得る．

次に，G の部分群 H（G はアーベル群ゆえ，$H \triangleleft G$ である．）に対して，G/H を考える．このとき，$G/H = \langle gH \rangle$ であることを示す．$\supset$ は明らかゆえ，$\subset$ を示す．すると，任意の $xH \in G/H$ に対して，$x = g^m$ $(m \in \mathbb{Z})$ とすれば，

$$xH = g^m H = (gH)^m$$

であるから，直ちに $G/H \subset \langle gH \rangle$ であることが分かる．□

定義 2.30（**元の位数**）G を群とする．各 $g \in G$ に対して，$g^n = 1_G$ を満たす自然数 n が存在するとき，そのような n の最小値を g の**位数** (order) という．すなわち，

$$\min\{n \in \mathbb{N} \mid g^n = 1_G\}$$

が G の位数である．また，$g^n = 1_G$ を満たす自然数 n が存在しないとき，g の位数は ∞ であると定める．

G が加法群の場合は，各 $g \in G$ に対して，$ng = g + g + \cdots + g = 0$ となる自然数 n の最小値が g の位数である．

例 2.31 自然数 $n \geq 1$ に対して，1 の複素 6 乗根全体のなす乗法群 $\mathcal{U}_6$ を考える．このとき，$\exp\left(\frac{2\pi\sqrt{-1}}{6}\right), \exp\left(\frac{4\pi\sqrt{-1}}{6}\right)$ の位数はそれぞれ，6, 3 である．一方，加法群 $\mathbb{Z}$ においては，$x \neq 0$ なる任意の $x \in \mathbb{Z}$ に対して，x の位数は ∞ である．実際，任意の自然数 n に対して，$nx \neq 0$ である．

命題 2.32 G を群とし，$g \in G$ を位数が n の元とする．このとき，ある $m \in \mathbb{Z}$ に対して，$g^m = 1_G$ となれば，m は n の倍数である．

証明. 剰余の定理より，ある $q, r \in \mathbb{Z}$ で，$m = nq + r$ かつ，$0 \leq r < n$ となるものが存在する．このとき，

$$1 = g^m = g^{nq+r} = (g^n)^q g^r = g^r$$

であるから，もし $r \neq 0$ であれば，n の最小性に矛盾する．よって，$r = 0$ となり，m は n の倍数である．□

命題 2.33 G を有限群とし，$|G| = n$ とする．このとき，

(1) 任意の $g \in G$ に対して，g の位数は n の約数である．

(2) $g \in G$ の位数が n であれば，$G = \langle g \rangle$．すなわち，G の位数と等しいような位数を持つ元が存在すれば G は巡回群である．

証明. (1) g の位数を m とする．このとき，

$$\langle g \rangle = \{1, g, g^2, \ldots, g^{m-1}\}$$

である．実際，$\supset$ は明らかである．一方，任意の $x \in \langle g \rangle$ とすると，ある整数 $k \in \mathbb{Z}$ が存在して $x = g^k$ と書ける．このとき，k を m で割ったときの商を q，余りを r とすると，$0 \leq r \leq m-1$ であり，

$$x = g^k = g^{mq+r} = (g^m)^q g^r = g^r \in \text{右辺}$$

となる．よって，$|\langle g \rangle| = m$ となるので，ラグランジュの定理より，m は n の約数である．

(2) g の位数が n とする．このとき，

$$\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$$

であるが，$|G| = n$ であるから，$\langle g \rangle$ は G に一致しなければならない．□

命題 2.34 G を群とし，$g \in G$ とする．このとき，g の（元としての）位数は，部分群 $\langle g \rangle$ の（群としての）位数に等しい．

証明. (1) g の位数が ∞ の場合．この場合は，任意の相異なる整数 $m, n \in \mathbb{Z}$ に対して，$g^m \neq g^n$ である．実際，$m > n$ とし，$g^m = g^n$ 仮定とすると，両辺に g^{-n} を乗じて，$g^{m-n} = 1$ を得る．これは，

g の位数が ∞ であることに矛盾する．したがって，

$$\langle g \rangle = \{1, g^{\pm 1}, g^{\pm 2}, g^{\pm 3}, \ldots\}$$

となり，$\langle g \rangle$ は（可算）無限個の元を含む．

(2) g の位数が $n \in \mathbb{N}$ の場合．このとき，命題 2.33 の (2) で述べたように，$|\langle g \rangle| = n$ である．□

命題 2.35 G を有限群とし，G の位数は素数 p であるとする．このとき，G は巡回群である．

証明. G の位数は 2 以上であるから，G には単位元以外の元 g が存在する．このとき，g が生成する部分群 $\langle g \rangle$ を考えるとこの部分群の位数は p の約数でなければならない．すなわち，1 または p である．特に，$1, g \in \langle g \rangle$ であるから $\langle g \rangle$ の位数は 1 ではない．よって，$|\langle g \rangle| = p$ となり，命題 2.33 より求める結果を得る．□

次に，巡回群の生成元の形や，生成元の個数について考えよう．

命題 2.36 G を g が生成する位数 n の巡回群とする．このとき，任意の $m \in \mathbb{Z}$ に対して，g^m の位数は $\dfrac{n}{\gcd(m,n)}$ である．ここで，$\gcd(m,n)$ は m と n の最大公約数を表す．

証明. $d = \gcd(m,n)$ とおき，$n = dn'$, $m = dm'$ とおくと，$\gcd(m', n') = 1$ である．このとき，

$$(g^m)^{\frac{n}{d}} = g^{\frac{mn}{d}} = g^{dm'n'} = (g^n)^{m'} = 1_G$$

となる．そこで，ある $1 \leq k < n/d = n'$ に対して，$(g^m)^k = 1_G$ となったとする．すると，g の位数は n であるから，ある $l \in \mathbb{Z}$ が存在して，$km = ln$ となる．これに，$n = dn'$, $m = dm'$ を代入して，$km' = ln'$ を得る．$\gcd(m', n') = 1$ であるから，$m' | l$ である．すなわち，ある $q \in \mathbb{Z}$ が存在して，$l = qm'$ とかける．よって，$k = qn'$ となる．これは $1 \leq k < n'$ に矛盾である．ゆえに，任意の $1 \leq k < n'$ に対して $(g^m)^k \neq 1_G$ である．したがって，g^m の位数は，$n/\gcd(m,n)$ である．□

この命題の系として，次の有益な結果を得る．

系 2.37 G を位数 n の巡回群とし，$G=\langle g\rangle$ とする．

(1) 整数 $m\in\mathbb{Z}$ に対して，G の部分群 $H=\langle g^m\rangle$ を考える．このとき，

$$H=G \iff \gcd(m,n)=1$$

が成り立つ．すなわち，g^m が G 全体を生成するのは m が G の位数 n と互いに素なときに限る．

(2) 位数 n の有限巡回群の生成元は全部で $\varphi(n)$ 個ある．ここで，$\varphi(n)$ はオイラー関数[25) を表す．

[25) オイラー関数については，本書の付録を参照されたい．

注意 2.38 1 の複素 6 乗根全体のなす群 $\mathcal{U}_6=\langle g\rangle$，($g=\exp\left(\frac{2\pi\sqrt{-1}}{6}\right)$) を考える．このとき，$0\leq m\leq 5$ に対して，g^m が $\mathcal{U}_6$ を生成するのは $m=1,5$ の場合のみである．

補題 2.39 G をアーベル群とし，$a,b\in G$ とする．a,b の位数をそれぞれ m,n とし，$\gcd(m,n)=1$ であるとする．このとき，ab の位数は mn である．

証明. まず，$(ab)^{mn}=a^{mn}b^{mn}=(a^m)^n(b^n)^m=1_G$ である．そこで，ある $1\leq k<mn$ に対して，$(ab)^k=1_G$ となったとする．両辺を m 乗すると，$(ab)^{km}=1_G$ より，$b^{km}=1_G$ を得る．b の位数は n なので，ある $l\in\mathbb{Z}$ が存在して $km=ln$ となるが，$\gcd(m,n)=1$ ゆえ $m|l$ である．すなわち，ある $q\in\mathbb{Z}$ が存在して，$l=mq$ とかける．よって，$k=qn$ となる．

したがって，$(ab)^k=1_G$ において $k=qn$ を代入すると，$a^{qn}=1_G$ となる．同様の議論により，$q=mr$ となる $r\in\mathbb{Z}$ が存在し，結局 $k=mnr$ を得る．これは $1\leq k<mn$ に矛盾である．よって，ab の位数は mn である．□

命題 2.29 とラグランジュの定理より，有限巡回群 G の任意の部分群は巡回群で，その位数は G の位数の約数になることが分かる．逆に，次のことが成り立つ．

命題 2.40 G を位数 n の有限巡回群とする．このとき，任意の n の約数 $m\in\mathbb{N}$ に対して，位数が m の部分群が一意的に存在する．

証明. $G=\langle g\rangle$ とする．g の位数は n である．今，$n=mt$ とおく

とき，$H := \langle g^t \rangle$ なる G の部分群を考える．H の位数が m になることを示そう．そのためには，g^t の位数が m になることを示せばよい．まず，明らかに，$(g^t)^m = g^{mt} = g^n = 1_G$ である．一方，$0 \leq m' < m$ なる整数 $m' \geq 0$ に対して，$(g^t)^{m'} = 1_G$ となったとすると，$tm' < tm = n$ かつ，$g^{tm'} = 1_G$ となるので，これは n の最小性に反する．したがって，g^t の位数は m である．

次に，G の位数 m の部分群は H しかないことを示す．そこで，H' を位数が m の G の部分群とし，$H = H'$ となることを示す．H' は巡回群なので $H' = \langle g^s \rangle$ なる，$0 \leq s \leq n-1$ が存在する．このとき，上と同様の議論により，g^s の位数は m である．すなわち，$g^{sm} = 1_G$ である．よって，命題 2.32 により，ある $k \in \mathbb{Z}$ が存在して，$sm = kn$ となる．したがって，$n = mt$ であるから，$s = kt$ である．これにより，

$$H' = \{1, g^{kt}, g^{2kt}, \ldots, g^{(m-1)kt}\} \subset H$$

であることが分かる．ところが，H も H' もともに位数が m の部分群であるから，$H' = H$ でなければならない．□

系 2.41 G を位数 n の有限巡回群とする．このとき，G の部分群の個数は n の正の約数の個数に一致する．

命題 2.40 と系 2.41 により，有限巡回群の任意の部分群が特徴づけられたことになる．まだあまり実感が湧かないかもしれないが，これはかなり強力なことを主張している．一般に，与えられた有限群の部分群にどのようなものがどれだけあるかを完全に決定することは非常に難しい．

注意 2.42 1 の複素 12 乗根たちのなす群 $\mathcal{U}_{12}$ で例にとってみよう．1 の 2 乗根や 3 乗根は，もちろん 1 の 12 乗根であるから $\mathcal{U}_2 \subset \mathcal{U}_{12}$，$\mathcal{U}_3 \subset \mathcal{U}_{12}$ となっている．他に，$\mathcal{U}_{12}$ の部分群がどれだけあるかというと，12 のすべての正の約数を考えて，全部で

$$\mathcal{U}_1 = \{1\},\ \mathcal{U}_2 = \{\pm 1\},\ \mathcal{U}_3,\ \mathcal{U}_4,\ \mathcal{U}_6,\ \mathcal{U}_{12}$$

の 6 個であることが分かる．

2.4 部分群の例

この節では，これまでに述べた群の部分群になっているもので，比較的扱いやすいものの例やその性質についていくつか解説する．初学者には多少敷居が高くなってしまうようなものもあるので，もし余裕がないようであれば，最初は交代群の節以外を読み飛ばしても後で困ることはない．

2.4.1 交代群

対称群の重要な部分群である交代群について考えよう．そこでまず，対称群の各元に対して符号と呼ばれるものを定義しよう．自然数 $n \geq 2$ に対して，n 個の変数 $X_1, \ldots, X_n$ とそれらの多項式

$$D = D(X_1, \ldots, X_n) := \prod_{1 \leq i < j \leq n} (X_i - X_j)$$

を，$X_1, \ldots, X_n$ の**差積** (difference product) という．置換 $\sigma \in \mathfrak{S}_n$ に対して

$$\sigma D = D(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) := \prod_{1 \leq i < j \leq n} (X_{\sigma(i)} - X_{\sigma(j)})$$

とおく．一般に，σD は，$X_1, \ldots, X_n$ のうち，異なる 2 つの変数の差全体の積になっているから，符号の違いを無視すれば，σD は D に等しい．すなわち，

$$\sigma D = \pm D$$

となる．そこで，$\sigma D = D$ のとき，σ を**偶置換** (even permutation) といい，$\sigma D = -D$ のとき，σ を**奇置換** (odd permutation) という．さらに，写像 $\mathrm{sgn} : \mathfrak{S}_n \to \{\pm 1\}$ を

$$\mathrm{sgn}(\sigma) = \begin{cases} 1, & \sigma \text{が偶置換} \\ -1, & \sigma \text{が奇置換} \end{cases}$$

で定める．この sgn を**符号関数** (signature function) または，単に**符号** (signature) という．定義から明らかに，

$$\sigma D = \mathrm{sgn}(\sigma) D$$

が成り立つ．また，符号が満たす重要な性質として以下のものがある．

補題 2.43 (1) $\sigma, \tau \in \mathfrak{S}_n$ に対して，

$$\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\ \mathrm{sgn}(\tau)$$

(2) $\sigma \in \mathfrak{S}_n$ に対して，

$$\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma)$$

証明. (1) については，

$$\begin{aligned}\mathrm{sgn}(\sigma\tau)D = (\sigma\tau)D = \sigma(\tau D) = \sigma(\mathrm{sgn}(\tau)D) = \mathrm{sgn}(\tau)(\sigma D)\\ = \mathrm{sgn}(\tau)\mathrm{sgn}(\sigma)D\end{aligned}$$

より明らか．

(2) (1) より，$\mathrm{sgn}(\sigma)\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(1_{\mathfrak{S}_n}) = 1$ であるので，これより直ちに得られる．□

さて，$X = \{1, 2, \ldots, n\}$ の中の相異なる m 個の文字 $a_1, \ldots, a_m$ に対して，

$$\sigma(b) = \begin{cases} a_{i+1}, & b = a_i,\ 1 \leq i < m, \\ a_1, & b = a_m, \\ b, & b \neq a_i,\ 1 \leq i \leq m, \end{cases}$$

なる置換 σ が定義される．これを，$(a_1\, a_2\, \cdots\, a_m)$ と表す．この型の置換を，長さが m の**巡回置換** (cyclic permutation) という．特に，長さが 2 の巡回置換を**互換** (transposition) という．すなわち，互換とはある二つの文字（これを i と j とする.）を入れ換えて，それ以外の文字は動かさないような X の置換

$$\begin{pmatrix} i & j \\ j & i \end{pmatrix}$$

のことである．

定理 2.44 n 次対称群 $\mathfrak{S}_n$ において，

(1) 互換は奇置換である．

(2) 任意の置換は互換の積として表される．ここで，単位元 $1_{\mathfrak{S}_n}$ は 0 個の置換の積と考える．すなわち，対称群は互換で生成される．

証明． (1) まず，$\sigma = (1\,2)$ の場合を考えよう．すると，任意の $m \geq 3$ に対して，

$$\sigma(X_1 - X_m)(X_2 - X_m) = (X_2 - X_m)(X_1 - X_m)$$

であるから，

$$D = \prod_{1 \leq i < j \leq n} (X_i - X_j) = (X_1 - X_2)D'$$

とすると，$\sigma D' = D'$ であり，

$$\sigma D = (X_2 - X_1)D'$$

となる．したがって，$\sigma D = -D$ となり，$\mathrm{sgn}((1\,2)) = -1$ を得る．

次に，任意の $\sigma = (i\,j)$ に対して，$\tau = (1\,i)(2\,j)$ とすると，$\sigma = \tau(1\,2)\tau^{-1}$ であるから

$$\mathrm{sgn}((i\,j)) = \mathrm{sgn}(\tau)\,\mathrm{sgn}((1\,2))\,\mathrm{sgn}(\tau^{-1}) = -1$$

を得る．

(2) n に関する帰納法で示す．$n = 2$ のときは，$\mathfrak{S}_2 = \{1_{\mathfrak{S}_2}, (1\,2)\}$ であるから明らか．そこで，$n \geq 3$ とし，$n-1$ のとき主張が正しいとする．任意の $\sigma \in \mathfrak{S}_n$ をとる．もし，$\sigma(n) = n$ であれば，σ は $n-1$ 個の文字の置換であると考えられるので，帰納法の仮定より，σ は互換の積として表せる．一方，$\sigma(n) \neq n$ のときは，ある $1 \leq i \leq n-1$ に対して $\sigma(i) = n$ となっており，

$$\sigma = \begin{pmatrix} n & \sigma(n) \\ \sigma(n) & n \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & n-1 & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) & \cdots & \sigma(n-1) & n \end{pmatrix}$$

である．このとき，

$$\sigma' := \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & n-1 & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) & \cdots & \sigma(n-1) & n \end{pmatrix}$$

は $n-1$ 個の文字の置換であると考えられるので，帰納法の仮定よ

り σ' は互換の積として表せる．ゆえに，σ も互換の積で書ける．以上より，帰納法が進む．□

系 2.45 n 次対称群 $\mathfrak{S}_n$ の元 σ に対して，σ が偶数個の互換の積で書ければ偶置換であり，奇数個の互換の積で書ければ奇置換である．

注意 2.46 任意の置換は有限個の互換の積で書ける．しかしながら，与えられた置換を互換の積で書く方法は一般に一通りではない．例えば次のような例がある．

$$(1\,3\,2) = (1\,2)(1\,3) = (1\,3)(2\,3)$$

である．

対称群 $\mathfrak{S}_n$ において互換 $\tau_1, \ldots, \tau_k$ の積を $\sigma = \tau_1 \cdots \tau_k$ とおくとき，

$$\sigma^{-1} = \tau_k \tau_{k-1} \cdots \tau_1$$

である．したがって，$\sigma \in \mathfrak{S}_n$ を偶置換とすると σ^{-1} も偶置換となる．また，明らかに，$\mathfrak{S}_n$ の単位元 $1_{\mathfrak{S}_n}$ は偶置換である．ゆえに，$\mathfrak{S}_n$ の偶置換全体の集合を $\mathfrak{A}_n$ とすれば[26)]，$\mathfrak{A}_n$ は $\mathfrak{S}_n$ の部分群である．これを，n 次の**交代群** (alternating group) という．特に，任意の $\tau \in \mathfrak{S}_n$ と任意の $\sigma \in \mathfrak{A}_n$ に対して，

$$\mathrm{sgn}(\tau\sigma\tau^{-1}) = (\mathrm{sgn}\tau)(\mathrm{sgn}\sigma)(\mathrm{sgn}\tau^{-1}) = \mathrm{sgn}\sigma = 1$$

であるから，$\tau\sigma\tau^{-1} \in \mathfrak{A}_n$ である．すなわち，$\mathfrak{A}_n$ は $\mathfrak{S}_n$ の正規部分群である．

26) $\mathfrak{A}$ はドイツ装飾大文字の A.

補題 2.47 n 次対称群 $\mathfrak{S}_n$ において奇置換全体の集合を $\mathfrak{O}_n$ とおくと[27)]，$|\mathfrak{O}_n| = |\mathfrak{A}_n|$ である．

27) $\mathfrak{O}$ はドイツ装飾大文字の O.

証明. $\tau \in \mathfrak{S}_n$ を互換とし固定する．このとき，写像 $f : \mathfrak{A}_n \to \mathfrak{O}_n$ を $\sigma \mapsto \tau\sigma$ によって定める．すると f は全単射である．実際，任意の奇置換 $\xi \in \mathfrak{O}_n$ に対して，$\sigma = \tau\xi$ とおくと σ は偶置換であり，$f(\sigma) = \tau\sigma = \tau^2\xi = \xi$ となるので f は全射．一方，$\sigma, \sigma' \in \mathfrak{A}_n$ に対して，$f(\sigma) = f(\sigma')$ となったとすると，$\tau\sigma = \tau\sigma'$ より $\sigma = \sigma'$ となることが分かる．したがって，f は単射である．よって，f は全単

射となり求める結果を得る．□

系 2.48 $n \geq 2$ に対して，$\mathfrak{A}_n$ は位数 $n!/2$ の有限群である．

証明. $|\mathfrak{S}_n| = n!$ であり，$|\mathfrak{S}_n| = |\mathfrak{O}_n| + |\mathfrak{A}_n| = 2|\mathfrak{A}_n|$ となることから明らか．□

定理 2.49 $n \geq 2$ に対して，

(1) $\mathfrak{S}_n$ は $n-1$ 個の互換

$$(1\,2),\ (1\,3),\ \ldots,\ (1\,n)$$

で生成される．

(2) $\mathfrak{A}_n$ は $n-2$ 個の長さ 3 の巡回置換

$$(1\,2\,3),\ (1\,2\,4),\ \ldots,\ (1\,2\,n)$$

で生成される．

証明. (1) 一般に，対称群は互換 $(i\,j)$ たちで生成される．もし，$i,j \neq 1$ であれば，$(i\,j) = (1\,i)(1\,j)(1\,i)$ と書けるのでこれより直ちに求める結果を得る．

(2) (1) より，$\mathfrak{A}_n$ の各元は $(1\,i)(1\,j)$ なる形の元の積として表せることが分かる．特に $i \neq j$ のとき，

$$(1\,i)(1\,j) = \begin{cases} (1\,j\,2) = (1\,2\,j)^{-1}, & i = 2,\ j \neq 1, 2 \\ (1\,2\,i), & j = 2,\ i \neq 1, 2 \\ (1\,2\,i)(1\,2\,j)^{-1}, & i, j \neq 1, 2 \end{cases}$$

となるので，求める結果を得る．□

補題 2.50 n 次対称群 $\mathfrak{S}_n$ において，長さ m の巡回置換 $(a_1\,a_2\,\cdots\,a_m)$ を考える．このとき，

$$(a_1\,a_2\,\cdots\,a_m) = (a_1\,a_m)(a_1\,a_{m-1})\cdots(a_1\,a_2)$$

が成り立つ．したがって，

$$(a_1\,a_2\,\cdots\,a_m) \in \mathfrak{A}_n \iff m \text{ が奇数}$$

となる．

証明. 前半は具体的に計算すればよい．後半は前半より直ちに従う．
□

2.4.2　可換環上の特殊線型群

R を可換環とする．自然数 $n \geq 1$ に対して，$\mathrm{GL}(n,R)$ の部分集合

$$\mathrm{SL}(n,R) := \{A \in \mathrm{GL}(n,R) \mid \det A = 1\} \subset \mathrm{GL}(n,R)$$

を考える．このとき，$\mathrm{SL}(n,R)$ は $\mathrm{GL}(n,R)$ の正規部分群になる．実際，$\det E_n = 1$ であるから，$E_n \in \mathrm{SL}(n,R)$ となり，$\mathrm{SL}(n,R) \neq \emptyset$．また，任意の $A, B \in \mathrm{SL}(n,R)$ に対して，$\det AB = (\det A)(\det B) = 1$ および，$\det A^{-1} = (\det A)^{-1} = 1$ となるので，$AB, A^{-1} \in \mathrm{SL}(n,R)$ である．したがって，$\mathrm{SL}(n,R)$ は $\mathrm{GL}(n,R)$ の部分群となる．この $\mathrm{SL}(n,R)$ を R 上の n 次の**特殊線型群** (special linear group) という．

一方，任意の $A \in \mathrm{SL}(n,R)$ と任意の $B \in \mathrm{GL}(n,R)$ に対して，

$$\det(BAB^{-1}) = (\det B)(\det A)(\det B)^{-1} = \det A = 1$$

となるので，$BAB^{-1} \in \mathrm{SL}(n,R)$ である．すなわち，$\mathrm{SL}(n,R)$ は $\mathrm{GL}(n,R)$ の正規部分群である．

2.4.3　$\mathbb{Z}$ 上のハイゼンベルグ群

この項で扱うハイゼンベルグ群は有限群ではないが，線型代数で学んだことが応用でき，群の生成元やそれらを用いた各元の一意的な表示を考察し理解を深めるための格好の題材であると思われるので取り上げることにした．大部分は Magnus[15] によった．

n を 2 以上の自然数とする．$\mathrm{SL}(n,\mathbb{Z})$ のある部分群について考察する．n 次の下三角行列

$$A = \begin{pmatrix} 1 & & O & & O \\ a_{21} & 1 & & \ddots & \\ a_{31} & a_{32} & \ddots & & O \\ \vdots & & \ddots & \ddots & \\ a_{n1} & a_{n2} & \cdots & a_{n,n-1} & 1 \end{pmatrix} \tag{2.1}$$

(ここで, 各 a_{ij} $(1 \leq j < i \leq n)$ は整数) に対して, $\det A = 1$ であるから, このような行列全体の集合を $\Lambda_n(\mathbb{Z})$ とおくと, $\Lambda_n(\mathbb{Z}) \subset \mathrm{SL}(n, \mathbb{Z})$ である. また, $E_n \in \Lambda_n(\mathbb{Z})$ である.

任意の $A = (a_{ij})$, $B = (b_{ij}) \in \Lambda_n(\mathbb{Z})$ に対して, $AB \in \Lambda_n(\mathbb{Z})$ となる. 実際, $C = AB = (c_{ij})$ とおくと

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

であるので, a_{ij}, b_{ij} がすべて整数であれば, c_{ij} も整数である. また, 任意の $1 \leq i < j \leq n$ をとるとき, 各 $1 \leq k \leq i$ に対して, $b_{kj} = 0$ であり, 各 $i < k \leq n$ に対して, $a_{ik} = 0$ であるので, $c_{ij} = 0$ である. 一方, $1 \leq i \leq n$ とする. 同様に, 各 $1 \leq k < i$ に対して $b_{kj} = 0$ であり, 各 $i < k \leq n$ に対して $a_{ik} = 0$ である. さらに, $k = i$ のとき, $a_{ii} = b_{ii} = 1$ ゆえ $c_{ii} = 1$ である. したがって, $C \in \Lambda_n(\mathbb{Z})$ であることが分かる.

次に, 任意の $A = (a_{ij}) \in \Lambda_n(\mathbb{Z})$ に対して, $A^{-1} \in \Lambda_n(\mathbb{Z})$ である. 実際, $\det A = 1$ であるから, $A^{-1} = \widetilde{A}$ である. $\widetilde{A} = (A_{ji})$ とする. 任意の $1 \leq i \leq n$ に対して, $A_{\langle ii \rangle} \in \Lambda_{n-1}(\mathbb{Z})$ であるから, $A_{ii} = \det A_{\langle ii \rangle} = 1$. 一方, 任意の $1 \leq i < j \leq n$ に対して, $A_{ji} = (-1)^{j+i} \det A_{\langle ji \rangle}$ である. ここで, $A_{\langle ji \rangle}$ は下三角行列であり, 対角成分の i 番目から $j-1$ 番目まではすべて 0 である. よって, $\det A_{\langle ji \rangle} = 0$ となり, $A_{ji} = 0$ を得る. したがって, $A^{-1} = \widetilde{A} \in \Lambda_n(\mathbb{Z})$ となる.

以上より, $\Lambda_n(\mathbb{Z})$ は $\mathrm{SL}(n, \mathbb{Z})$ の部分群になることが分かる. これを $\mathbb{Z}$ 上の n 次の**ハイゼンベルグ群** (Heisenberg group) という. $\Lambda_n(\mathbb{Z})$ の生成元について考えよう.

$P(i, j; 1)$ を, 対角成分と (i, j) 成分が 1 で, それ以外は 0 である

ような基本行列とする．各 $1 \leq j < i \leq n$ および，任意の整数 a, b に対して，

$$P(i,j;a)P(i,j;b) = P(i,j;a+b)$$

が成り立つ．実際，行列の基本変形を思い出すと $P(i,j;a)P(i,j;b)$ は，$P(i,j;b)$ の第 j 行を a 倍して第 i 行に加えたものである．$P(i,j;b)$ の第 j 行は，対角成分が 1 でそれ以外は 0 であるから，第 j 行を a 倍したものは

$$\begin{pmatrix} 0 & \cdots & 0 & \overset{j}{a} & 0 & \cdots & 0 \end{pmatrix}$$

となる．ゆえに，$P(i,j;a)P(i,j;b) = P(i,j;a+b)$ である．よって，帰納法により任意の自然数 $m \geq 1$ に対して，$P(i,j;1)^m = P(i,j;m)$ となることが分かる．さらに，

$$P(i,j;1)P(i,j;-1) = P(i,j;0) = E_n$$

であるから，$P(i,j;1)^{-1} = P(i,j;-1)$ である．したがって，同様の議論により，任意の整数 a に対して $P(i,j;1)^a = P(i,j;a)$ である．

次に，任意の $2 \leq i \leq n$ および，任意の整数の組 $a_{i1}, a_{i2}, \ldots, a_{i,i-1}$ に対して，

$$D(i;a_{i1},\ldots,a_{i,i-1}) = \begin{array}{c} \\ \\ \\ i \\ \\ \end{array}\begin{pmatrix} E & & & & \\ O & \ddots & & & \\ O & & E & & \\ a_{i1} & \cdots & a_{i,i-1} & 1 & \\ O & \cdots & \cdots & O & E \end{pmatrix}$$

とおくと，

$$D(i;a_{i1},\ldots,a_{i,i-1}) = P(i,1;1)^{a_{i1}}P(i,2;1)^{a_{i2}}\cdots P(i,i-1;1)^{a_{i,i-1}}$$

となることが分かる．実際，各 $1 \leq k \leq i-1$ に対して，$P(i,1;a_{i1})P(i,2;a_{i,2})\cdots P(i,k;a_{i,k})$ は，第 i 行が

$$\begin{array}{ccccccc} 1 & 2 & \cdots & k & \cdots & i & \\ \end{array}$$
$$\begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{ik} & O & 1 & O \end{pmatrix}$$

であり，その他の行は対角成分のみが 1 でそれ以外が 0 となる行列であることを k についての帰納法で示す．$k=1$ のときは明らか．そこで，$k \geq 1$ とする．このとき，

$$P(i,1;a_{i1})\cdots P(i,k;a_{i,k})P(i,k+1;a_{i,k+1})$$

は，$P(i,1;a_{i1})\cdots P(i,k;a_{i,k})$ の第 i 列を $a_{i,k+1}$ 倍したものを第 $k+1$ 列に足したものである．ところが，帰納法の仮定から，$P(i,1;a_{i1})\cdots P(i,k;a_{i,k})$ の第 i 列は基本ベクトル $\boldsymbol{e}_i$ であるから，$P(i,1;a_{i1})\cdots P(i,k;a_{i,k})P(i,k+1;a_{i,k+1})$ の第 i 行は

$$\begin{array}{cccccccc} 1 & 2 & \cdots & k & k+1 & \cdots & i & \\ \end{array}$$
$$\begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{ik} & a_{i,k+1} & O & 1 & O \end{pmatrix}$$

であり，その他の行は対角成分のみが 1 でそれ以外が 0 となる行列である．よって帰納法が進む．

このとき，(2.1) の形で与えられる任意の行列 A に対して，

$$A = D(2;a_{21})D(3;a_{31},a_{32})\cdots D(n;a_{n1},\ldots,a_{n,n-1}) \qquad (2.2)$$

となる．実際，上式右辺は単位行列 E_n から出発して，順に

- $\boldsymbol{e}_2$ を a_{21} 倍したものを第 1 列に加える．
- $\boldsymbol{e}_3$ を a_{31} 倍したものを第 1 列に加える．
- $\boldsymbol{e}_3$ を a_{32} 倍したものを第 2 列に加える．
- $\boldsymbol{e}_4$ を a_{41} 倍したものを第 1 列に加える．
- $\vdots$

なる操作を施して出来上がる行列であり，これは A にほかならない．特に，このような表示は A に対して一意的であることも分かる．

以上により，

$$\Lambda_n(\mathbb{Z}) = \langle P(i,j;1) \,|\, 1 \leq j < i \leq n \rangle$$

であり，$\Lambda_n(\mathbb{Z})$ の各元 A は (2.2) により

$$A = P(2,1;1)^{a_{21}} \cdot (P(3,1;1)^{a_{31}} P(3,2;1)^{a_{32}}) \cdots$$
$$\cdots (P(n,1;1)^{a_{n1}} P(n,2;1)^{a_{n2}} \cdots P(n,n-1;1)^{a_{n,n-1}})$$

なる形に一意的に表されることが分かる．これを，生成系

$$\{P(i,j;1) \mid 1 \leq j < i \leq n\}$$

に関する**標準形** (normal formal) という．

このような，生成系とその標準形の例として，正二面体群については，例 2.12 で与えた．しかしながら一般に，与えられた群の生成元を求めることは時として甚だ困難であり，仮に生成元を求められたとしても，それらを用いて各元を一意的に表す方法（標準形）を与えることはさらに難しい．

2.5 問題

問題 2.1 G を群，H, K を G の部分群とする．このとき，$H \cup K$ が G の部分群とはならないような例を挙げよ．

解答． G として整数全体のなす加法群 $\mathbb{Z}$ を考える．このとき，2 の倍数全体 $2\mathbb{Z}$，および 3 の倍数全体 $3\mathbb{Z}$ は $\mathbb{Z}$ の部分群である．ここで，$2\mathbb{Z} \cup 3\mathbb{Z}$ を考える．すると，$2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ であるが，$5 = 2 + 3 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$ であるので，$2\mathbb{Z} \cup 3\mathbb{Z}$ は $\mathbb{Z}$ の部分群ではない．
□

問題 2.2 G をアーベル群とするとき，$Z(G) = G$ であることを示せ．

解答． 任意の $g \in G$ をとる．任意の $s \in G$ に対して，G はアーベル群であるから $gs = sg$ が成り立つ．よって，$g \in Z(G)$ である．つまり，$G \subset Z(G)$．逆の包含関係は明らかである．□

問題 2.3 自然数 $n \geq 2$ に対して，n 次対称群 $\mathfrak{S}_n$ の中心を求めよ．

解答． $n = 2$ のとき，$\mathfrak{S}_2$ はアーベル群であるから $Z(\mathfrak{S}_2) = \mathfrak{S}_2$．以下，$n \geq 3$ とする．そこで，$\sigma \neq 1_{\mathfrak{S}_n}$ なる任意の $\sigma \in \mathfrak{S}_n$ を考

える．すると，ある $1 \le i \le n$ で $\sigma(i) \ne i$ となるものが存在する．$j = \sigma(i)$ とおく．一方，$n \ge 3$ より，$k \ne i, j$ なる $1 \le k \le n$ が存在する．このとき，

$$(\sigma(j\,k))(i) = j, \quad ((j\,k)\sigma)(i) = k$$

であるから，$\sigma(j\,k) \ne (j\,k)\sigma$ であることが分かる．すなわち，$\sigma \notin Z(\mathfrak{S}_n)$ である．したがって，$Z(\mathfrak{S}_n) = \{1_{\mathfrak{S}_n}\}$ を得る．□

問題 2.4 自然数 $n \ge 2$ に対して，n 次特殊線型群 $\mathrm{SL}(n, \mathbb{Z})$ の中心を求めよ．

解答． $A = (a_{ij}) \in Z(\mathrm{SL}(n, \mathbb{Z}))$ とする．任意の $1 \le i \ne j \le n$ に対して，$a_{ij} = 0$ である．実際，$k \ne i$ なる $1 \le k \le n$ に対して，$P(k, i; 1)A = AP(k, i; 1)$ であるから，(k, j) 成分を比較して，$a_{kj} + a_{ij} = a_{kj}$ となり，$a_{ij} = 0$ を得る．（ここで，$P(i, j; 1)$ は (i, j) 成分と対角成分が 1 でそれ以外の成分がすべて 0 であるような $\mathrm{SL}(n, \mathbb{Z})$ の行列である．）したがって，A は対角行列となる．

次に，任意の $1 \le i \ne j \le n$ に対して，

$$P(i, j) = (\boldsymbol{e}_1, \ldots \boldsymbol{e}_{i-1}, \boldsymbol{e}_j, \boldsymbol{e}_{i+1}, \ldots, \boldsymbol{e}_{j-1}, \boldsymbol{e}_i, \boldsymbol{e}_{j+1}, \ldots, \boldsymbol{e}_n)$$

なる行列を考える．$P(i, j)$ は第 i 行 (列) と第 j 行 (列) を入れ換える基本変形に対応する基本行列である．このとき，$P(i, j)A = AP(i, j)$ の (i, j) 成分を比較して，$a_{ii} = a_{jj}$ となることが分かる．したがって，A はスカラー行列 aE_n なる形であることが分かる．すると，行列式を考えることで $a^n = 1$ であることが分かる．特に，a は整数であるから $a = \pm 1$ を得る．

したがって，

$$Z(\mathrm{SL}(n, \mathbb{Z})) = \begin{cases} \{\pm E_n\}, & n \text{ が偶数のとき}, \\ \{E_n\}, & n \text{ が奇数のとき}, \end{cases}$$

となる．□

問題 2.5 整数全体のなす加法群 $\mathbb{Z}$ を考える．$n \in \mathbb{Z}$ とする．この

とき，以下を示せ．

(1) $n = \pm 1$ のとき，n は $\mathbb{Z}$ の生成元である．
(2) $n \neq \pm 1$ のとき，n は $\mathbb{Z}$ の生成元ではない．

解答. (1) 任意の $m \in \mathbb{Z}, m \neq 0$ に対して，

$$m = \begin{cases} 1 + 1 + \cdots + 1, & \text{if} \quad m > 0 \\ (-1) + (-1) + \cdots + (-1), & \text{if} \quad m < 0 \end{cases}$$

とかける．ここで，上式右辺の和は $|m|$ 回足すことを意味している．よって，$n = 1$ は生成元である．まったく同様にして，$n = -1$ も生成元であることが分かる．
(2) $n \neq \pm 1$ とする．このとき，$\langle n \rangle = n\mathbb{Z}$ であり，特に $\pm 1 \notin n\mathbb{Z}$ であるから，n は $\mathbb{Z}$ の生成元ではない．□

問題 2.6 $n \geq 2$ を自然数とする．n 次対称群 $\mathfrak{S}_n$ は互換

$$\sigma_i := \begin{pmatrix} i & i+1 \\ i+1 & i \end{pmatrix}, \quad 1 \leq i \leq n-1$$

たちで生成されることを示せ．

解答. 対称群は互換で生成されるから，任意の互換が σ_i たちの積で書けることを示せばよい．そこで，$i \neq j$ なる任意の $1 \leq i, j \leq n$ に対して，$\sigma := (i\,j)$ とする．このとき，$i > j$ としても一般性を失わない．すると，

$$\sigma = \sigma_{i-1}\sigma_{i-2} \cdots \sigma_{j+1}\sigma_j\sigma_{j+1} \cdots \sigma_{i-2}\sigma_{i-1}$$

となるので，これより求める結果を得る．□

問題 2.7 $n \geq 2$ を自然数とし，K を体とする．このとき，一般線型群 $\mathrm{GL}(n, K)$ は基本行列たちで生成されることを示せ．

解答. 任意の $A \in \mathrm{GL}(n, K)$ に対して基本変形を施すことで

$$PAQ = \begin{pmatrix} E_r & O \\ O & O \end{pmatrix}$$

なる形に変形できる．ここで，P は A に施した行基本変形に対応する基本行列たちの積であり，Q は A に施した列基本変形に対応する基本行列たちの積である．このとき，両辺の行列式の値を見ることで，$r=n$ でなければならないことが分かる．もしそうでないとすると $r<n$ となり，右辺の行列式が 0 になる．ゆえに，$A=P^{-1}Q^{-1}$ とかける．これより求める結果を得る．□

問題 2.8 加法群 $\mathbb{Q}$ は無限生成群であることを示せ．

解答． $\mathbb{Q}$ が有限生成だと仮定し，$S=\{s_1,s_2,\ldots,s_r\}$ をその生成系とする．いま，各 $1\leq i\leq r$ に対して，s_i を既約分数 p_i/q_i，$(q_i\geq 1)$ に表示し，分母を素因数分解する．このときに現れる素数全体の集合を S' とおくと，明らかに，$\langle S\rangle\subset\langle S'\rangle\subset\mathbb{Q}$ であるから，$\langle S'\rangle=\mathbb{Q}$ である．さて，p を S' に含まれない素数[28] とする．このとき，$1/p\in\langle S'\rangle$ であるから，

[28] 素数は無限に存在するので必ずとれる．

$$\frac{1}{p}=a_1\frac{1}{p_1}+a_2\frac{1}{p_2}+\cdots+a_r\frac{1}{p_r},\quad a_i\in\mathbb{Z}$$

を得る．通分して整理すると，

$$p_1p_2\cdots p_r=p\times\text{整数}$$

なる形になるが，これは素因数分解の一意性に反する．ゆえに，$\mathbb{Q}$ は無限生成群である．□

問題 2.9 正の有理数全体 $\mathbb{Q}^+$ は通常の乗法により群をなす．このとき，素数全体はこの乗法群 $\mathbb{Q}^+$ の生成系であることを示せ．また，$\mathbb{Q}^+$ は無限生成群であることを示せ．

解答． (1) 任意の $x\in\mathbb{Q}^+$ に対して，x は既約分数として p/q（p,q は自然数．）なる形に書ける．（x が自然数のときは，$x=x/1$ である．）このとき，p と q の素因数分解をそれぞれ $p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$，$q_1^{f_1}q_2^{f_2}\cdots q_s^{f_s}$ とすれば，

$$x=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}q_1^{-f_1}q_2^{-f_2}\cdots q_s^{-f_s}$$

である．したがって，乗法群 $\mathbb{Q}^+$ は素数全体で生成される．

一方，$\mathbb{Q}^+$ が有限生成だとして，$S=\{s_1,s_2,\ldots,s_r\}$ をその生成

系とする．いま，各 $1 \leq i \leq r$ に対して，s_i を既約分数に表示し，分母分子を素因数分解する．このときに現れる素数全体の集合を S' とおくと，明らかに，$\langle S \rangle \subset \langle S' \rangle \subset \mathbb{Q}^+$ であるから，$\langle S' \rangle = \mathbb{Q}^+$ である．さて，p を S' に含まれない素数とする．このとき，$p \in \langle S' \rangle$ であるから，

$$p = \frac{p_1^{e_1} p_2^{e_2} \cdots p_r^{e_s}}{q_1^{f_1} q_2^{f_2} \cdots q_s^{f_t}}, \quad p_i, q_j \in S'$$

と書ける．よって，$pq_1^{f_1} q_2^{f_2} \cdots q_s^{f_t} = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_s}$ となるが，これは素因数分解の一意性に反する．ゆえに，$\mathbb{Q}^+$ は無限生成である．□

問題 2.10 G を群，$K \subset H \subset G$ を部分群の列とする．$[G:H]$ と $[H:K]$ がともに有限であれば，$[G:K]$ も有限で，

$$[G:K] = [G:H][H:K]$$

が成り立つことを示せ．

解答． $[G:H] = r$，$[H:K] = s$ とおき，G の H による剰余類分割と，H の K による剰余類分割をそれぞれ

$$G = \bigcup_{i=1}^{r} g_i H, \quad H = \bigcup_{j=1}^{s} h_j K$$

とする．このとき，

$$G = \bigcup_{i=1}^{r} \bigcup_{j=1}^{s} g_i h_j K$$

が G の K による剰余類分割である．実際，$g_i h_j K \cap g_k h_l K \neq \emptyset$ とすると，ある $x \in g_i h_j K \cap g_k h_l K$ が存在する．このとき，$xH = g_i H = g_k H$ となるので，$i = k$ である．よって，$h_j K \cap h_l K \neq \emptyset$ となる．そこで，$y \in h_j K \cap h_l K$ とするとき，$yK = h_j K = h_l K$ となるので $j = l$ を得る．したがって，$(i,j) \neq (k,l)$ である．すなわち，上の分割は互いに交わりのない K の剰余類たちによる分割である．よって，$[G:K] = rs$ となる．□

問題 2.11 G を部分群，H, K を指数有限な G の部分群とする．このとき，$H \cap K$ も指数有限であることを示せ．

解答. まず，$[G:H\cap K]=[G:H][H:H\cap K]$ であるから，$[H:H\cap K]<\infty$ であることを示せばよい．

そこで，剰余類の集合の間の写像 $f:H/(H\cap K)\to HK/K$ を $g(H\cap K)\mapsto gK$ によって定める．このとき，$a(H\cap K)=b(H\cap K)$ であれば，$b^{-1}a\in H\cap K\subset K$ であるから，$aK=bK$ となり f は well-defined [29] である．さらに，任意の $a\in HK$ に対して $aK\in HK/K$ を考える．すると，ある $h\in H$ と $k\in K$ が存在して $a=hk$ となる．このとき，$aK=(hk)K=hK=f(h(H\cap K))$ となるので f は全射である．また，$a,b\in H$ に対して $f(a(H\cap K))=f(b(H\cap K))$ と仮定すると，$aK=bK$ より，$b^{-1}a\in K$ となる．したがって，$b^{-1}a\in H\cap K$ となり $a(H\cap K)=b(H\cap K)$ を得る．つまり f は単射である．

以上より，$[H:H\cap K]=|H/(H\cap K)|=|HK/K|$ であることが分かる．一方，$[G:K]=[G:HK][HK:K]$ であるから，$[HK:K]=|HK/K|<\infty$ である．これより求める結果を得る．□

[29] 矛盾なく整合的に定義されているという意味である．一般に，写像は，定義域の各元に対して値域の元が一意的に対応していなければならない．このことが成り立つと確認できるときに，「その対応は写像として well-defined である」といういい方をする．

問題 2.12 G を群，H を位数が n であるような G の部分群とする．G の位数 n の部分群が H の他に存在しないとき，H は G の正規部分群であることを示せ．

解答. 任意の $g\in G$ に対して，$gHg^{-1}=H$ となることを示せばよい．まず，gHg^{-1} は G の部分群になる．実際，$1_G=g1_Gg^{-1}\in gHg^{-1}$ であり，任意の $x,y\in gHg^{-1}$ に対して $x=ghg^{-1}$, $y=gh'y^{-1}$, $(h,h'\in H)$ とおくと，

$$xy=g(hh')g^{-1},\quad x^{-1}=gh^{-1}g^{-1}\in gHg^{-1}$$

である．一方，写像 $\varphi_g:G\to G$ を $x\mapsto gxg^{-1}$ によって定めると φ_g は単射である．実際，$x,y\in G$ に対して，$gxg^{-1}=gyg^{-1}$ と仮定すれば $x=y$ を得る．ゆえに，$gHg^{-1}=\varphi_g(H)$ の位数は n である．仮定により，位数 n の部分群は H のみであるから，$gHg^{-1}=H$ を得る．□

問題 2.13 G を有限群とし，H を部分群とする．

(1) G の H による左（右）剰余類の集合を

$$\mathcal{L} := \{gH \mid g \in G\}, \quad \mathcal{R} := \{Hg \mid g \in G\}$$

とおく．このとき，$|\mathcal{L}| = |\mathcal{R}|$ であることを示せ．

(2) $[G : H] = 2$ であれば，H は G の正規部分群であることを示せ．

解答． (1) まず，G の各左剰余類 gH に対して，$|gH| = |H|$ である．写像 $f : gH \to Hg$ を $gh \mapsto hg$ で定めると，f は全単射である．実際，f の全射性は構成から明らか．また，$h, h' \in H$ に対して，$f(gh) = f(gh')$ とすると，$hg = h'g$ となるので $h = h'$ を得る．ゆえに，f は単射である．よって，H の右剰余類 Hg に含まれる元の個数は gH のそれに等しく，したがって，$|Hg| = |H|$ を得る．

このとき，G の H による左剰余類の個数 $|\mathcal{L}|$ は $[G : H] = |G|/|H|$ であるが，同様にして H による右剰余類の個数 $|\mathcal{R}|$ も $|G|/|H|$ となることが分かる．よって，$|\mathcal{L}| = |\mathcal{R}|$ である．

(2) G の左剰余類の分解を $G = H \cup gH$ とすると，G の右剰余類の分解は $G = H \cup Hg'$ なる形になる．ここで，$g \notin H$ であるから，$g \in Hg'$ であり，したがって，$Hg' = Hg$ である．さらに，上の各剰余類分解は共通部分が空集合であるような直和であるので，$gH = Hg$ でなければならない．

さて，任意の $\sigma \in G$ に対して，σ は $\sigma \in H$ か，もしくは $\sigma \in gH = Hg$ である．$\sigma \in H$ のときは明らかに $\sigma H = H\sigma$ である．$\sigma \in gH = Hg$ のときは，ある $h, h' \in H$ が存在して，$\sigma = gh = h'g$ とかける．このとき，$\sigma H = (gh)H = gH = Hg = H(h'g) = H\sigma$ となる．ゆえに，H は G の正規部分群である．□

問題 2.14 G を群とする．このとき，任意の自然数 $n \geq 1$ に対して，

$$G(n) := \langle x^n \mid x \in G \rangle$$

は G の正規部分群であることを示せ．

解答． 任意の $g \in G$ に対して，$gG(n)g^{-1} \subset G(n)$ を示す．そこで，任意の $x \in G(n)$ とすると，

$$x = x_1^n x_2^n \cdots x_m^n, \quad x_i \in G$$

とかける．このとき，

$$gxg^{-1} = (gx_1g^{-1})^n(gx_2g^{-1})^n \cdots (gx_mg^{-1})^n, \quad gx_ig^{-1} \in G$$

となるので，$gxg^{-1} \in G(n)$ である．これより求める結果を得る．□

問題 2.15 位数 12 の巡回群の部分群の個数を求めよ．

解答． 12 の正の約数 $1, 2, 3, 4, 6, 12$ であり，これらの約数の数だけ部分群が存在するので全部で 6 個である．□

問題 2.16 1 の複素 8 乗根全体のなす群 $\mathcal{U}_8 = \langle g \rangle$, $(g = \exp(\frac{2\pi\sqrt{-1}}{8}))$ に対して，$\mathcal{U}_8$ の生成元をすべて求めよ．

解答． $0 \leq m \leq 7$ に対して，g^m が生成元となるのは $(m, 8) = 1$ の場合で，$m = 1, 3, 5, 7$ のときである．□

問題 2.17 複素平面内の単位円周

$$S := \{\exp(\theta\sqrt{-1}) \in \mathbb{C} \,|\, \theta \in \mathbb{R}\} \subset \mathbb{C}$$

を考える．S は $\mathbb{C}$ の乗法により乗法群になる．このとき，S の任意の有限部分群は巡回群であることを示せ．

解答． G を S の任意の有限部分群とする．G の各元を偏角が $0 \leq \theta < 2\pi$ の範囲にあるように

$$g = \exp(\theta\sqrt{-1}), \quad 0 \leq \theta_g < 2\pi$$

と表す．このとき，1 と異なる G の元で，偏角が最も小さい元を x とする．このとき，$G = \langle x \rangle$ である．実際，ある $g \in G$ で $g \notin \langle x \rangle$ なるものが存在するとすると，ある $m \in \mathbb{Z}, m \geq 0$ で

$$m\theta_x < \theta_g < (m+1)\theta_x$$

となるものが存在する．このとき，$y = gx^{-m} \in G$ であり，$0 < \theta_y = \theta_g - m\theta_x < \theta_x$ となるので，θ_x の最小性に矛盾である．よって，$g \in \langle x \rangle$，すなわち，$G = \langle x \rangle$ となる．□

3 群の同型概念

本章では，群論で最も大切な概念である同型について学ぶ．大雑把にいって，二つの群が同型であるというのは，定義や見かけ等は異なるが両者の間に一対一対応があり，その対応で群の積が同じものとみなせるということである．このような概念は応用上も非常に有益であり，与えられた群がどのような群と同型になるのかどうかを決定する問題は群論の根幹をなす重要な問題である．

3.1 準同型定理と同型定理

ベクトル空間の間の線型写像や，位相空間の間の連続写像のように，積という演算を兼ね備えた群の間の写像を考えるときは，その構造を保つような特別な写像を考えるのが理論上有益である．これを準同型写像という．本節では，準同型写像についての性質を解説する．

定義 3.1 (**準同型写像, 同型写像**) G, H を群とする．写像 $f : G \to H$ が，任意の $x, y \in G$ に対して $f(xy) = f(x)f(y)$ を満たすとき，f を**準同型写像** (homomorphism) という．

特に，準同型写像 $f : G \to H$ が全単射であるとき，f を**同型写像** (isomorphism) という．また，このような同型写像が存在するとき，G と H は**同型** (isomorphic) であるといい，$G \cong H$ と表す．

注意 3.2 $f : G \to H$ が同型写像のとき，f の逆写像 $f^{-1} : H \to G$

も準同型写像（したがって，同型写像）である．実際，任意の $a,b\in H$ に対して $a=f(x), b=f(y)$ とおくと，

$$f^{-1}(ab)=f^{-1}(f(x)f(y))=f^{-1}(f(xy))=xy=f^{-1}(a)f^{-1}(b)$$

が成り立つ．

例 3.3 自然数 $n\geq 1$ に対して，1 の複素 n 乗根全体のなす巡回群 $\mathcal{U}_n$ と，加法群 $\mathbb{Z}$ の剰余群 $\mathbb{Z}/n\mathbb{Z}$ を考える．写像 $f:\mathbb{Z}/n\mathbb{Z}\to\mathcal{U}_n$ を

$$[a]_n\mapsto\exp\left(\frac{2a\pi\sqrt{-1}}{n}\right)$$

によって定める．すると，f は well-defined である．実際，$[a]_n=[b]_n$ とすると，ある整数 $m\in\mathbb{Z}$ が存在して，$a-b=nm$ と書ける．このとき，

$$\begin{aligned}f([b]_n)&=\exp\left(\frac{2b\pi\sqrt{-1}}{n}\right)=\exp\left(\frac{2(a+mn)\pi\sqrt{-1}}{n}\right)\\&=\exp\left(\frac{2a\pi\sqrt{-1}}{n}\right)\left(\exp\left(\frac{2n\pi\sqrt{-1}}{n}\right)\right)^m=\exp\left(\frac{2a\pi\sqrt{-1}}{n}\right)\\&=f([a]_n)\end{aligned}$$

が成り立つ．

次に，f が全単射であることを示そう．任意の $z\in\mathcal{U}_n$ に対して，ある整数 $0\leq a\leq n-1$ が存在して $z=\exp\left(\frac{2a\pi\sqrt{-1}}{n}\right)$ と書けるので，$f([a]_n)=z$ である．よって，f は全射．一方，$[a]_n,[b]_n\in\mathbb{Z}/n\mathbb{Z}$ に対して，$f([a]_n)=f([b]_n)$ と仮定すると，$\exp\left(\frac{2a\pi\sqrt{-1}}{n}\right)=\exp\left(\frac{2b\pi\sqrt{-1}}{n}\right)$ となる．よって，$\exp\left(\frac{2(a-b)\pi\sqrt{-1}}{n}\right)=1$ となるので，$2(a-b)\pi/n$ は 2π の整数倍である．よって，$n|(a-b)$ となり，$[a]_n=[b]_n$ を得る．

最後に，f が準同型写像であることを示そう．任意の $[a]_n,[b]_n\in\mathbb{Z}/n\mathbb{Z}$ に対して，

$$\begin{aligned}f([a]_n+[b]_n)=f([a+b]_n)&=\exp\left(\frac{2(a+b)\pi\sqrt{-1}}{n}\right)\\&=\exp\left(\frac{2a\pi\sqrt{-1}}{n}\right)\exp\left(\frac{2b\pi\sqrt{-1}}{n}\right)=f([a]_n)f([b]_n)\end{aligned}$$

となるので，f は加法群 $\mathbb{Z}/n\mathbb{Z}$ から乗法群 $\mathcal{U}_n$ への準同型写像であ

る．以上により，f は同型写像となり，$\mathbb{Z}/n\mathbb{Z} \cong \mathcal{U}_n$ であることが分かる．

注意 3.4 単に二つの群が「同型」といっても，あくまで抽象的な群として両者は"同じような型をしている"のであって，"まったく同じものとみなす"というわけではない．例えば，$\mathcal{U}_n$ と $\mathbb{Z}/n\mathbb{Z}$ は群としては同型であるが，$\mathcal{U}_n$ には乗法群としての良さ（有用性，利便性など）があり，$\mathbb{Z}/n\mathbb{Z}$ には加法群としての良さがある．群のどのような性質に注目するかによって，両者の相性を見きわめて使い分けることもしばしば重要であろう．

補題 3.5 G, H を群とし，$f : G \to H$ を準同型写像とする．このとき，

(1) $f(1_G) = 1_H$ である．
(2) 各 $x \in G$ に対して，$f(x^{-1}) = f(x)^{-1}$ が成り立つ．

証明. (1) $1_G \cdot 1_G = 1_G$ であるから，$f(1_G)f(1_G) = f(1_G \cdot 1_G) = f(1_G)$ となる．一方，$f(1_G) \in H$ であるから，逆元 $f(1_G)^{-1} \in H$ が存在する．これを上式の両辺に左から乗じて，$f(1_G) = 1_H$ を得る．
(2) 任意の $x \in G$ に対して，$xx^{-1} = 1_G$ であるから，$f(xx^{-1}) = f(x)f(x^{-}) = f(1_G) = 1_H$ となる．同様に，$x^{-1}x = 1_G$ より $f(x^{-1})f(x) = 1_H$ であることも分かる．ゆえに，H における逆元の一意性から，$f(x^{-1}) = f(x)^{-1}$ である．□

補題 3.6 G, H, K を群とし，$f : G \to H$, $f' : H \to K$ を準同型写像とする．このとき，合成写像 $f' \circ f : G \to K$ は準同型写像である．

証明. 任意の $x, y \in G$ に対して，

$$
\begin{aligned}
(f' \circ f)(xy) &= f'(f(xy)) = f'(f(x)f(y)) \\
&= f'(f(x))f'(f(y)) = (f' \circ f)(x)(f' \circ f)(y)
\end{aligned}
$$

となるので明らか．□

定義 3.7（像と核） G, H を群とし，$f : G \to H$ を準同型写像とす

る．このとき，

$$\{f(g) \in H \mid g \in G\} \subset H$$

を f の**像** (image) といい，$f(G)$, $\mathrm{Im}(f)$ などと表す．また，

$$\{g \in G \mid f(g) = 1_H\} \subset G$$

を f の**核** (kernel) といい，$\mathrm{Ker}(f)$ と表す．

命題 3.8 G, H を群とし，$f : G \to H$ を準同型写像とする．このとき，以下が成り立つ．

(1) $\mathrm{Im}(f)$ は H の部分群である．
(2) $\mathrm{Ker}(f)$ は G の正規部分群である．

証明. (1) まず，命題 3.5 の (1) より，$1_H \in \mathrm{Im}(f)$ であるから，$\mathrm{Im}(f)$ は空ではない．任意の $a, b \in \mathrm{Im}(f)$ に対して $a = f(x), b = f(y)$ なる $x, y \in G$ が存在する．このとき，準同型写像の定義から $ab = f(x)f(y) = f(xy) \in \mathrm{Im}(f)$ である．また，各 $a \in \mathrm{Im}(f)$ に対して $a = f(x)$ なる $x \in G$ をとると，命題 3.5 の (2) より，$a^{-1} = f(x)^{-1} = f(x^{-1}) \in \mathrm{Im}(f)$ である．ゆえに，$\in \mathrm{Im}(f)$ は H の部分群である．

(2) $1_G \in \mathrm{Ker}(f)$ であるから，明らかに $\mathrm{Ker}(f)$ は空ではない．また，任意の $x, y \in \mathrm{Ker}(f)$ に対して，$f(xy) = f(x)f(y) = 1_H$, $f(x^{-1}) = f(x)^{-1} = 1_H$ であるから，$xy, x^{-1} \in \mathrm{Ker}(f)$ である．よって，$\mathrm{Ker}(f)$ は G の部分群である．さらに，任意の $g \in G$，および任意の $x \in \mathrm{Ker}(f)$ に対して，$f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)1_H f(g)^{-1} = 1_H$ であるから，$gxg^{-1} \in \mathrm{Ker}(f)$ となる．したがって，$\mathrm{Ker}(f)$ は G の正規部分群である．□

以下の命題は，与えられた準同型写像が単射かどうかを調べるには，その核に注目すればよいことを示している．

命題 3.9 G, H を群とし，$f : G \to H$ を準同型写像とする．このとき，

$$f\text{ が単射} \iff \mathrm{Ker}(f) = \{1_G\}$$

が成り立つ．

証明. ($\Longrightarrow$) f を単射とする．$\{1_G\} \subset \mathrm{Ker}(f)$ は明らかなので，$\mathrm{Ker}(f) \subset \{1_G\}$ を示す．任意の $g \in \mathrm{Ker}(f)$ とする．このとき，$f(g) = 1_H$ であるが，補題3.5より $f(1_G) = 1_H$ でもある．よって，f の単射性から $g = 1_G$ を得る．

($\Longleftarrow$) $g, g' \in G$ に対して，$f(g) = f(g')$ と仮定する．すると，

$$f(g'g^{-1}) = f(g')f(g^{-1}) = f(g')f(g)^{-1} = 1_H$$

となるので，$g'g^{-1} \in \mathrm{Ker}(f) = \{1_H\}$ である．ゆえに，$g'g^{-1} = 1$，すなわち $g' = g$ である．□

一般に，ある剰余群からの準同型写像を自然に構成しようとするとき，以下の補題はきわめてよく用いられる．

補題 3.10 G, H を群，$f : G \to H$ を準同型写像とする．N を G の正規部分群で，$f(N) = \{1_H\}$ であるとする．すなわち，$N \subset \mathrm{Ker}(f)$ とする．このとき，$\overline{f} : G/N \to H$ を

$$\overline{f}(gN) := f(g)$$

と定めると，$\overline{f}$ は well-defined で群準同型写像となる．

証明. 任意の $g' \in gN$ に対して，$\overline{f}(g'N) = f(g)$ となることを示す．そこで，$g' \in gN$ であるからある $n \in N$ が存在して，$g' = gn$ と書ける．よって，$\overline{f}(g'N) = f(g') = f(gn) = f(g)f(n) = f(g)$ を得る．したがって，$\overline{f}$ は well-defined である．$\overline{f}$ が群準同型であることは，任意の $xN, yN \in G/N$ に対して，

$$\overline{f}(xN \cdot yN) = \overline{f}(xyN) = f(xy) = f(x)f(y) = \overline{f}(xN)\overline{f}(yN)$$

となることから分かる．□

定義 3.11 補題3.10において得られた $\overline{f} : G/N \to H$ を，f から**誘導された準同型** (homomorpshim induced by f) という．

以下の定理は群論の中で最も基本的でかつ重要な定理のうちの一つであり，種々の局面で使いこなせるようになるべき定理である．本節では，後に第1, 2, 3同型定理を解説するが，極端にいえば準同

型定理を適当にいい換えたものに過ぎず，準同型定理をしっかり理解していればいつでも証明を再構成できよう．

定理 3.12（準同型定理） G, H を群とし，$f : G \to H$ を準同型写像とする．このとき，$G/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$ が成り立つ．特に，f が全射であれば，$G/\mathrm{Ker}(f) \cong H$ である．

証明. 補題3.10より，f は自然な準同型写像 $\overline{f} : G/\mathrm{Ker}(f) \to H$ を誘導する．特に，定義から分かるように，この $\overline{f}$ の像は $\mathrm{Im}(f)$ に一致しているので，値域を $\mathrm{Im}(f) \subset H$ に制限すれば，$\overline{f} : G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ は全射準同型写像である．これが単射であることを示す．そのために，$g\mathrm{Ker}(f) \in \mathrm{Ker}(\overline{f})$ と仮定する．このとき，

$$1_H = \overline{f}(g\mathrm{Ker}(f)) = f(g)$$

であるから，$g \in \mathrm{Ker}(f)$ であることが分かる．すなわち，$g\mathrm{Ker}(f) = \mathrm{Ker}(f)$ となり，これは $G/\mathrm{Ker}(f)$ の単位元であるから，命題3.9より，$\overline{f}$ は単射である．したがって，$\overline{f}$ は同型写像となり，求める結果を得る．□

補題 3.13 G, H を群とし，$f : G \to H$ を全射準同型とする．K を H の部分群とするとき，$f^{-1}(K)$ は G の部分群である．

証明. まず，$f(1_G) = 1_H \in K$ であるので，$1_G \in f^{-1}(K)$ となり，$f^{-1}(K) \neq \emptyset$．次に，任意の $x, y \in f^{-1}(K)$ に対して，

$$f(xy) = f(x)f(y) \in K, \quad f(x^{-1}) = f(x)^{-1} \in K$$

となるので，$xy, x^{-1} \in f^{-1}(K)$ を得る．よって，$f^{-1}(K)$ は G の部分群である．□

定義 3.14 G を群，N を G の正規部分群とする．自然な商写像 $\pi : G \to G/N$ は準同型写像である．実際，任意の $x, y \in G$ に対して，

$$\pi(xy) = (xy)N = (xN)(yN) = \pi(x)\pi(y)$$

が成り立つ．この π を**自然な全射準同型写像** (natural surjective

homomorphism)，**商準同型写像** (quotient homomorphism) などという．

定理 3.15（第 1 同型定理） G, H を群とし，$f: G \to H$ を全射準同型とする．N を H の正規部分群とするとき，以下が成り立つ．

(1) $f^{-1}(N)$ は G の正規部分群.
(2) $G/f^{-1}(N) \cong H/N$

証明. (1) 補題3.13より，$f^{-1}(N)$ は G の部分群であるから，$f^{-1}(N)$ が G の元の共役で閉じていることを示せばよい．任意の $x \in f^{-1}(N)$ と任意の $g \in G$ をとる．$f(x) \in N$ であり，N は正規部分群であるから

$$f(gxg^{-1}) = f(g)f(x)f(g)^{-1} \in N$$

である．すなわち，$gxg^{-1} \in f^{-1}(N)$ である．

(2) $f: G \to H$ と自然な全射準同型写像 $\pi: H \to H/N$ の合成写像を $f': G \to H/N$ とおく．f も π も全射なので，f' も全射である．このとき，任意の $x \in f^{-1}(N)$ に対して，

$$f'(x) = \pi(f(x)) = (f(x))N = N$$

であるから，$f^{-1}(N) \subset \mathrm{Ker}(f')$ である．一方，任意の $x \in \mathrm{Ker}(f')$ に対して，上式と同様の議論により，$(f(x))N = N$ となるので，$f(x) \in N$ であることが分かる．つまり，$x \in f^{-1}(N)$ となり，$\mathrm{Ker}(f') \subset f^{-1}(N)$ となる．

以上より，$\mathrm{Ker}(f') = f^{-1}(N)$ となるので，準同型定理より求める結果を得る．□

定理 3.16（第 2 同型定理） G を群とし，K を G の部分群，N を G の正規部分群とする．このとき以下が成り立つ．

(1) $KN = \langle K, N \rangle$.
(2) N は KN の正規部分群であり，$K \cap N$ は K の正規部分群である.
(3) $K/(K \cap N) \cong KN/N$.

証明. (1) 任意の $x \in KN$ に対して，ある $k \in K$, $n \in N$ が存在

して $x = kn$ と書けるので，明らかに $x \in \langle K, N \rangle$．逆に，任意の $x \in \langle K, N \rangle$ とする．一般に，$k \in K$，$n \in N$ のとき $k^{-1} \in K$，$n^{-1} \in N$ であることに注意すると，ある $k_1, k_2, \ldots, k_m \in K$ とある $n_1, n_2, \ldots, n_m \in N$ が存在して，

$$x = k_1 n_1 k_2 n_2 \cdots k_m n_m$$

とかける．ただし，$k_1 = 1_G$ もしくは $n_m = 1_G$ でもよいものとする．

そこで，上の形の元が KN に属することを m についての帰納法で示そう．$m = 1$ のときは明らかである．そこで，$m > 1$ とし，$m - 1$ 以下のとき主張が成り立つと仮定する．このとき，帰納法の仮定により，

$$k_1 n_1 k_2 n_2 \cdots k_{m-1} n_{m-1} = kn$$

となるような，$k \in K$，$n \in N$ が存在する．すると，

$$x = knk_m n_m = kk_m(k_m^{-1} nk_m)n_m$$

であり，$kk_m \in K$，$(k_m^{-1} nk_m)n_m \in N$ であるから，$x \in KN$ となる．したがって帰納法が進むことが分かる．以上より，求める等式を得る．

(2) N は G の正規部分群であり，KN は G の部分群であるから $N \lhd KN$ は明らか．一方，$K \cap N$ は G の部分群であり，明らかに K に含まれているので，K の部分群でもある．また，任意の $k \in K$ と任意の $x \in K \cap N$ に対して，N は正規部分群であるから $kxk^{-1} \in N$ であり，K は群であるから $kxk^{-1} \in K$．したがって，$kxk^{-1} \in K \cap N$ となり，$K \cap N$ は K の正規部分群である．

(3) 包含写像 $K \hookrightarrow KN$[30] と自然な全射準同型 $\pi : KN \to KN/N$ の合成写像を $f : K \to KN/N$ とおく．すると f は全射である．実際，任意の $xN \in KN/N$ に対して，$x = kn$ となる $k \in K$，$n \in N$ が存在する．このとき，$xN = (kn)N = kN = (f(k))N$ となるので f は全射である．

次に，f の核を調べる．任意の $x \in K \cap N$ に対して，$f(x) = xN = N$ であるから，$x \in \mathrm{Ker}(f)$．よって，$K \cap N \subset \mathrm{Ker}(f)$．一方，任意の $x \in \mathrm{Ker}(f)$ に対して，$x \in K$ であり，$(f(x))N = xN = N$

30) 記号 $\hookrightarrow$ は単射である写像を意味するときに用いる．

であるから $x \in N$ であることも分かる．すなわち，$x \in K \cap N$ である．よって，$\mathrm{Ker}(f) \subset K \cap N$ となり，$\mathrm{Ker}(f) = K \cap N$ を得る．

以上より，準同型定理を用いて $K/(K \cap N) \cong KN/N$ であることが分かる．□

定理 3.17（対応原理） G を群とし，N を G の正規部分群とする．$\pi : G \to G/N$ を自然な全射準同型とする．

$$X := \{\mathcal{K} \mid \mathcal{K} \text{ は } G/N \text{ の部分群 }\}$$
$$Y := \{H \leq G \mid N \subset H\}$$

とおく．このとき，写像 $f : X \to Y$ を

$$f(\mathcal{K}) = \pi^{-1}(\mathcal{K})$$

によって定めると，f は全単射である．すなわち，G/N の部分群と，N を含む G の部分群たちは一対一に対応する．

証明． (1) f が well-defined であること．

f の像が Y に含まれていることを示す．すなわち，任意の $\mathcal{K} \leq G/N$ に対して，$N \subset \pi^{-1}(\mathcal{K})$ であることを示せばよい．すると，任意の $n \in N$ に対して，$\pi(n) = nN = N = 1_{G/N} \in \mathcal{K}$ であるから，$n \in \pi^{-1}(\mathcal{K})$．よって，$N \subset \pi^{-1}(\mathcal{K})$ である．

(2) f が全単射であること．

まず，全射性について考える．任意の $H \in Y$ に対して，N は H の正規部分群であるから剰余群 H/N を考えることができる．そこで，包含写像 $H \hookrightarrow G$ と自然な全射準同型写像 $\pi : G \to G/N$ の合成写像を $\iota : H \to G/N$ とおくと，$N = \mathrm{Ker}(\iota)$ である．よって，準同型定理より ι は単射準同型写像 $\bar{\iota} : H/N \to G/N$ を誘導する．このとき，$\mathcal{K} = \mathrm{Im}(\bar{\iota})$ とおくと，$\pi^{-1}(\mathcal{K}) = H$ である．実際，任意の $h \in H$ に対して，

$$\pi(h) = hN = (\iota(h))N = \bar{\iota}(hN) \in \mathcal{K}$$

であるから，$H \subset \pi^{-1}(\mathcal{K})$．逆に，任意の $x \in \pi^{-1}(\mathcal{K})$ とすると，$xN = \pi(x) \in \mathcal{K} = \mathrm{Im}(\bar{\iota})$ であるから，ある $hN \in H/N$ が存在して，$\bar{\iota}(hN) = xN$ となっている．$\bar{\iota}(hN) = hN \in G/N$ であること

に注意して，$hN = xN$ となる．すなわち，ある $n \in N$ が存在して，$x = hn$ と書ける．$N \subset H$ であるから，$x \in H$ であることが分かる．よって，$\pi^{-1}(\mathcal{K}) \subset H$ となり，$\pi^{-1}(\mathcal{K}) = H$ を得る．したがって，$f(\mathcal{K}) = H$ となり，f は全射である．

次に，f が単射であることを示そう．$\mathcal{K}_1, \mathcal{K}_2 \in X$ とし，$f(\mathcal{K}_1) = f(\mathcal{K}_2)$ と仮定する．すると，$\pi^{-1}(\mathcal{K}_1) = \pi^{-1}(\mathcal{K}_2)$ であるが，両辺に π を施すことで，$\mathcal{K}_1 = \mathcal{K}_2$ を得る．よって，f は単射である．□

注意 3.18 定理 3.17 において，任意の $H \in Y$ に対して，準同型写像 $\bar{\iota}: H/N \to G/N$ は単射であった．つまり，H/N と $\mathrm{Im}(\bar{\iota})$ は同型である．さらに，この準同型写像は自然な包含写像 $H \hookrightarrow G$ から誘導されているものであるので，$\bar{\iota}$ を通して H/N と $\mathrm{Im}(\bar{\iota})$ を同一視してもほとんど問題ない．ゆえに，以下特に断らない限り常にこのような同一視を考え，$H/N \leq G/N$ とみなすことにする．

定理 3.19（第 3 同型定理） G を群とし，H, K を G の正規部分群とし，K を H の部分群とする．このとき，以下が成り立つ．

(1) K は H の正規部分群であり，（注意 3.18 の下で）H/K は G/K の正規部分群である．
(2) $(G/K)/(H/K) \cong G/H$.

証明. (1) K は G の正規部分群であり，H の部分群でもあるから，明らかに H の正規部分群である．一方，注意 3.18 で述べたように，H/K は G/K の部分群である．特に，任意の $hK \in H/K$ と任意の $gK \in G/K$ に対して，

$$(gK)(hK)(gK)^{-1} = (ghg^{-1})K \in H/K$$

となるので，$H/K \lhd G/K$ となる．

(2) $\pi : G \to G/H$ を自然な全射準同型写像とする．すると，$K \subset \mathrm{Ker}(\pi)$ であるから，補題 3.10 により π は全射準同型写像 $\bar{\pi}: G/K \to G/H$ を誘導する．このとき，$\mathrm{Ker}(\bar{\pi}) = H/K$ である．実際，$xK \in \mathrm{Ker}(\bar{\pi})$ とすると，$\bar{\pi}(xK) = H$ であり，$\bar{\pi}(xK) = xH$ であるから $xH = H$ となる．これは $x \in H$ を意味し，したがって $xK \in H/K$ であることが分かる．よって，$\mathrm{Ker}(\bar{\pi}) \subset H/K$.

逆に，任意の $hK \in H/K$ に対して，$\pi(hK) = hH = H$ となるので，$hK \in \mathrm{Ker}(\pi)$ となる．すなわち，$\mathrm{Ker}(\pi) \supset H/K$ となり，$\mathrm{Ker}(\pi) = H/K$ を得る．以上により，準同型定理から求める同型を得る．□

有限群においては，（そもそも位数が異なるので）真部分群が元の群と同型になることはないが，無限群の場合ではそうでないこともある．簡単な例を挙げておこう．加法群 $\mathbb{Z}$ を考える．自然数 $n \in \mathbb{Z}$ に対して，n の倍数全体のなす部分集合

$$n\mathbb{Z} := \{nr \in \mathbb{Z} \mid r \in \mathbb{Z}\} \subset \mathbb{Z}$$

は $\mathbb{Z}$ の部分群である．このとき，準同型写像 $f : \mathbb{Z} \to n\mathbb{Z}$ を $f(r) = (nr)$ によって定める．これが準同型写像になることは，任意の $r, s \in \mathbb{Z}$ に対して，

$$f(r+s) = n(r+s) = nr + ns = f(r) + f(s)$$

となることから明らか．さらに，全単射であることも以下のようにして分かる．まず，任意の $x \in n\mathbb{Z}$ に対して，$x = nr$ となる $r \in \mathbb{Z}$ が存在するので，$f(r) = x$ となる．つまり，f は全射．一方，$f(r) = 0$ とすると，$nr = 0$ より $r = 0$ となる．したがって，f は単射である．以上により，f は同型写像となる．

では次のようなことを考えてみよう．自然数 $n \geq 2$ に対して $n\mathbb{Z} \subset \mathbb{Z}$ を考える．$\mathbb{Z}$ の $n\mathbb{Z}$ による剰余群 $\mathbb{Z}/n\mathbb{Z}$ は位数 n の巡回群であった．一方，$n\mathbb{Z}$ は $\mathbb{Z}$ と同型であるから，$\mathbb{Z}/n\mathbb{Z}$ は $\mathbb{Z}/\mathbb{Z}$ と同型である．すなわち，位数 n の巡回群 $\mathbb{Z}/n\mathbb{Z}$ は位数 1 の自明な群に同型である．どの部分の議論が間違っているかお分かりになるだろうか．

3.2 直積群

この節では，与えられたいくつかの群から新しい群を構成する方法のうちの一つとして，直積なる操作を考える．これは，次節で考える有限アーベル群の構造定理を理解する上で必須の概念である．

定義 3.20 (直積群) G と H を群とする．このとき，直積集合 $G \times H$ に積を $(g,h),(g',h') \in G \times H$ に対して，

$$(g,h) \cdot (g',h') := (gg', hh')$$

によって定める．ここで，gg', hh' はそれぞれ，G, H における積である．

すると，$G \times H$ はこの積に関して群になる．実際，結合法則を満たすことは，上の演算は各成分ごとに群 G と H の演算を用いて定義されていることと，G と H において結合法則が成り立つことから容易に示される．単位元は $(1_G, 1_H)$ であり，(g,h) の逆元は (g^{-1}, h^{-1}) で与えられる．この群 $G \times H$ を G と H の**直積群** (direct product)，もしくは**外部直積** (external direct product) [31] という．

31) この表現はあまり使われない．本書では，以下で定める内部直積と区別したいときのみ用いる．

一般に，2 個以上の複数の群 $H_1, H_2, \ldots, H_n$ に対して[32]，その直積群 $H_1 \times H_2 \times \cdots \times H_n$ が

$$(h_1, h_2, \ldots, h_m) \cdot (h'_1, h'_2, \ldots, h'_m) := (h_1h'_1, h_2h'_2, \ldots, h_mh'_m)$$

によって同様に定義される．

32) 選択公理を仮定すれば，無限個の群の族 $\{H_\lambda\}_{\lambda \in \Lambda}$ でもよい．

明らかに，有限個の有限群 $H_1, H_2, \ldots, H_n$ に対して，

$$|H_1 \times H_2 \times \cdots \times H_n| = |H_1| \times |H_2| \times \cdots \times |H_n|$$

が成り立つ．

補題 3.21 有限個の群 $H_1, H_2, \ldots, H_n$ に対して，それらの直積群 $H_1 \times H_2 \times \cdots \times H_n$ を考える．各 $1 \leq i \leq n$ に対して，

$$(h_1, h_2, \ldots, h_n) \mapsto h_i$$

によって定まる，第 i 成分への自然な射影を $\mathrm{pr}_i : H_1 \times H_2 \times \cdots \times H_n \to H_i$ とおく．このとき，各 pr_i は全射準同型写像である．

証明. 任意の $1 \leq i \leq n$ をとって固定する．任意の $h \in H_i$ に対して，

$$\mathrm{pr}_i(1_{H_1}, \ldots, 1_{H_{i-1}}, h, 1_{H_{i+1}}, \ldots, 1_{H_n}) = h$$

であるから pr_i は全射である．

次に, 任意の $(h_1, h_2, \ldots, h_m), (h'_1, h'_2, \ldots, h'_m) \in H_1 \times H_2 \times \cdots \times H_n$ に対して,

$$\begin{aligned}
&\mathrm{pr}_i((h_1, h_2, \ldots, h_m)(h'_1, h'_2, \ldots, h'_m)) \\
&\quad = \mathrm{pr}_i((h_1h'_1, h_2h'_2, \ldots, h_mh'_m)) = h_ih'_i \\
&\quad = \mathrm{pr}_i((h_1, h_2, \ldots, h_m))\mathrm{pr}_i((h'_1, h'_2, \ldots, h'_m))
\end{aligned}$$

となるので, pr_i は準同型である. □

補題 3.22 G, H, K を群とする. このとき,

$$(G \times H) \times K \cong G \times (H \times K) \cong G \times H \times K$$

が成り立つ. すなわち, 群の直積は括弧の付け方によらず, 同型を除いて一意的に定まる.

証明. 写像 $f : (G \times H) \times K \to G \times H \times K$ を

$$((g, h), k) \mapsto (g, h, k), \quad g \in G,\ h \in H,\ k \in K$$

によって定める. 明らかに f は全単射である. f が準同型であることは

$$\begin{aligned}
f(((g, h),k)((g', h'), k')) &= f(((g, h)(g', h'), kk')) \\
&= f(((gg', hh'), kk') = (gg', hh', kk') \\
&= (g, h, k)(g', h', k') = f(((g, h), k))f(((g', h'), k'))
\end{aligned}$$

より従う. よって, $(G \times H) \times K \cong G \times H \times K$ を得る. $G \times (H \times K) \cong G \times H \times K$ も同様にして得られる. □

注意 3.23 上の補題では三つの群の直積を考えたが, 一般に, 任意個の群の直積に関して同様の主張が成り立つ.

さて, 外部直積はいくつかの別個の群を用いて構成されるものである. 一方で, ある群において, それに含まれるいくつかの部分群たちの外部直積が元の群と同型になるようなことがある. 以下これについて考える.

定義 3.24 (内部直積) G を群, $H_1, \ldots, H_n \leq G$ を部分群とし, こ

れらが以下の性質を満たすとする.

(I1) $G = H_1 H_2 \cdots H_n$.

(I2) (1) より, 任意の $g \in G$ に対して, ある $h_i \in H_i, 1 \leq i \leq n$ が存在して, $g = h_1 h_2 \cdots h_n$ と表すことができるが, このような表し方は一意的.

(I3) $1 \leq i, j \leq n$, $i \neq j$ に対して, H_i の各元と H_j の各元は交換可能.

このとき, G は $H_1, \ldots, H_n$ の**内部直積** (internal direct product) といい, $G = H_1 \dot{\times} \cdots \dot{\times} H_n$ [33] と表す.

[33] $\dot{\times}$ は $\times$ と区別するために用いた積を表す記号である.

定理 3.25 G を群, $H_1, \ldots, H_n \leq G$ を部分群とする. このとき, 以下は同値である.

$$G = H_1 \dot{\times} \cdots \dot{\times} H_n$$

$$\iff \begin{cases} (1)\ G = H_1 H_2 \cdots H_n, \\ (2)\ \text{任意の } 1 \leq i \leq n \text{ に対して } H_i \text{ は } G \text{ の正規部分群}, \\ (3)\ \text{任意の } 1 \leq i \leq n-1 \text{ に対して} \\ \qquad (H_1 H_2 \cdots H_i) \cap H_{i+1} = \{1_G\}. \end{cases}$$

証明. ($\Longrightarrow$) (1) が成り立つことは定義より明らか. (2) を示す. 任意の $h \in H_i$ と任意の $g \in G$ に対して, (I1) より, $g = h_1 h_2 \cdots h_n$ ($h_i \in H_i$) とかける. すると, (I3) より, $g = h_i h_1 \cdots h_{i-1} h_{i+1} \cdots h_n$ となる. このとき, (I3) を用いて

$$\begin{aligned} ghg^{-1} &= (h_i h_1 \cdots h_{i-1} h_{i+1} \cdots h_n)\, h\, (h_n^{-1} \cdots h_{i+1}^{-1} h_{i-1}^{-1} \cdots h_1^{-1} h_i^{-1}) \\ &= h_i h (h_1 \cdots h_{i-1} h_{i+1} \cdots h_n)\, (h_n^{-1} \cdots h_{i+1}^{-1} h_{i-1}^{-1} \cdots h_1^{-1}) h_i^{-1} \\ &= h_i h h_i^{-1} \in H_i \end{aligned}$$

となるので, $gH_i g^{-1} \subset H_i$ となる. すなわち, H_i は G の正規部分群である. 次に, (3) を示す. 任意の $1 \leq i \leq n-1$ をとって固定する. 任意の $x \in (H_1 H_2 \cdots H_i) \cap H_{i+1}$ に対して, $x \in H_1 H_2 \cdots H_i$ であるから, ある $h_1 \in H_1, \ldots, h_i \in H_i$ が存在して, $x = h_1 h_2 \cdots h_i$ とかける. すなわち,

$$1_{H_1} 1_{H_2} \cdots 1_{H_i}\, x\, 1_{H_{i+2}} \cdots 1_{H_n} = h_1 h_2 \cdots h_i\, 1_{H_{i+1}} 1_{H_{i+2}} \cdots 1_{H_n}$$

なる式を得る（$1_{H_j} = 1_G$ である.）が，(I2) により，このような表示は一意的であるから，各 $1 \leq j \leq i-1$ に対して $h_j = 1_{H_j}$ であり，$x = 1_{H_{i+1}}$ であることが分かる．したがって，$(H_1H_2 \cdots H_i) \cap H_{i+1} \subset \{1_G\}$ となる．逆の包含関係は明らかなので，求める等式を得る．

($\Longleftarrow$) (I1) が成り立つことは (1) より明らか．(I2) を示す．そこで，任意の $g \in G$ に対して，

$$g = h_1h_2 \cdots h_n = h'_1h'_2 \cdots h'_n, \quad h_i, h'_i \in H_i$$

となったと仮定する．すると，

$$h_n(h'_n)^{-1} = (h_1h_2 \cdots h_{n-1})^{-1}(h'_1h'_2 \cdots h'_{n-1})$$

となるが，左辺は H_n の元で，右辺は $H_1H_2 \cdots H_{n-1}$ の元であるから，両者は $H_1H_2 \cdots H_{n-1} \cap H_n$ の元である．よって，(3) よりこれは単位元に等しく，

$$h_n = h'_n, \quad h_1h_2 \cdots h_{n-1} = h'_1h'_2 \cdots h'_{n-1}$$

となる．以下帰納的に，$h_{n-1} = h'_{n-1}$, $h_{n-2} = h'_{n-2}$, ..., $h_1 = h'_1$ であることが示される．最後に, (I3) を示そう．そこで, $i < j$ なる i, j を固定し, 任意の $h_i \in H_i$, $h_j \in H_j$ をとる．このとき, $h := h_ih_jh_i^{-1}$ とおくと，(2) より $h \in H_j$ である．一方，$h_ih_j = (hh_ih^{-1})h$ であるから，(3) より，$h_i = hh_ih^{-1}$ かつ $h_j = h$ であることが分かる．すなわち，$h_ih_j = h_jh_i$ を得る．よって，H_i の各元と H_j の各元は交換可能である．□

定理 3.26 G を群，$H_1, \ldots, H_n \subset G$ を部分群とし，$G = H_1 \dot{\times} \cdots \dot{\times} H_n$ とする．このとき，

$$G \cong H_1 \times \cdots \times H_n$$

である．

証明. 同型写像を構成する．写像 $f : H_1 \times \cdots \times H_n \to G$ を

$$(h_1, h_2, \ldots, h_n) \mapsto h_1h_2 \cdots h_n$$

で定義する．すると，内部直積の性質 (I1) より f は全射でり，(I2) より f は単射であることが分かる．そこで，f が準同型写像であることを示そう．任意の $(h_1, h_2, \ldots, h_n), (h'_1, h'_2, \ldots, h'_n) \in H_1 \times \cdots \times H_n$ に対して逐次 (I3) を考えることで，

$$
\begin{aligned}
f((h_1,&h_2, \ldots, h_n)(h'_1, h'_2, \ldots, h'_n)) \\
&= f((h_1 h'_1, h_2 h'_2, \ldots, h_n h'_n)) = h_1 h'_1 h_2 h'_2 \, (h_3 h'_3 \cdots h_n h'_n) \\
&= h_1 h_2 h'_1 h'_2 \, (h_3 h'_3 \cdots h_n h'_n) \\
&= h_1 h_2 h_3 h'_1 h'_2 h'_3 \, (h_4 h'_4 \cdots h_n h'_n) \\
&= \cdots = (h_1 h_2 \cdots h_n)(h'_1 h'_2 \cdots h'_n) \\
&= f((h_1, h_2, \ldots, h_n)) f((h'_1, h'_2, \ldots, h'_n))
\end{aligned}
$$

を得る．以上より，f は同型写像であることが分かる．□

3.3 群の同型類

定義 3.27（同型類） 二つの群が同型であるという関係 $\cong$ は，群全体の集合族における同値関係になる．実際，任意の群 G に対して，G 上の恒等写像 $\mathrm{id}_G : G \to G$ [34] は同型写像であるから，$G \cong G$．次に，群 G と H に対して，$G \cong H$ とする．このとき，同型写像 $f : G \to H$ が存在するが，f の逆写像 $f^{-1} : H \to G$ は同型写像であるから，$H \cong G$．また，群 G, H, K に対して，$G \cong H$ かつ $H \cong K$ となったとする．このとき，同型写像 $f : G \to H$，$f' : H \to K$ が存在する．すると，これらの合成写像 $f' \circ f : G \to K$ も同型写像になるので，$G \cong K$ である．

一般に，群 G に対して，G と同型な群全体からなる同値類を G の**同型類** (isomorphism class) という．

[34] 任意の $g \in G$ に対して，$\mathrm{id}_G(g) = g$ なる写像のこと．

群論では，与えられた未知の群の同型類を決定すること（特に，よく知られている群の同型類に一致するかどうかを調べること）は非常に大切な問題である．この種の研究を行う際には，群の同型に関する不変量や性質（同型な群の間で変わらない何か．この「何か」は整数や実数のような数であったり，集合であったりすることもある）

を見つけることが大事である．以下では，これまでに述べた内容を用いて，群の同型に関して不変的な性質をいくつか解説しよう．中には自明なものもあるし，他にも挙げれば切りがないが，一度だけでいいので，必ずこのような訓練を経験しておくとよいと思う．

命題 3.28 G と H を同型な群とするとき，以下のことが成り立つ．

(1) G がアーベル群であれば，H もアーベル群．
(2) G が有限生成（または無限生成）であれば，H も有限生成（または無限生成）である．
(3) N を G の（正規）部分群とし，$f : G \to H$ を任意の同型写像とする．このとき，$f(N)$ は H の（正規）部分群であり，$[G : N] = [H : f(N)]$ である．
(4) G' と H' を同型な群とするとき，$G \times H \cong G' \times H'$ である．

証明. 以下，$f : G \to H$ を任意の同型写像として固定する．
(1) 任意の $x', y' \in H$ に対して，f の全射性から，ある $x, y \in G$ であって，$x' = f(x)$，$y' = f(y)$ となるものがとれる．このとき，

$$x'y' = f(x)f(y) = f(xy) = f(yx) = f(y)f(x) = y'x'$$

となるので，H はアーベル群である．

(2) G を有限生成とし，S を有限個の元からなる G の生成系とする．$f(S)$ が H の生成系であることを示そう．そこで，任意の $x \in H$ をとる．f は全射ゆえ，ある $x \in G$ が存在して，$x' = f(x)$ と書ける．一方，S は G の生成系であるから，x は

$$x = s_1^{e_1} s_2^{e_2} \cdots s_m^{e_m}, \quad s_i \in S,\ e_i = \pm 1$$

と書ける．このとき，

$$x' = f(x) = f(s_1^{e_1} s_2^{e_2} \cdots s_m^{e_m}) = f(s_1)^{e_1} f(s_2)^{e_2} \cdots f(s_m)^{e_m}$$

である．よって，H は $f(S)$ で生成される．f は単射であるから，$|f(S)| = |S|$ となり，H は有限生成である．

一方，G が無限生成であるとし，H が有限生成であると仮定する．このとき，f の逆写像 $f^{-1} : H \to G$ は同型写像であるから，上と

同様の議論により，G は有限生成となる．これは矛盾である．よって，H も無限生成となる．

(3) まず，$f(N)$ が H の正規部分群であることを示す．任意の $x' \in f(N)$ と任意の $h \in H$ に対して，ある $x \in N$ および $g \in G$ が存在して，$x' = f(x)$ 及 $h = f(g)$ となる．このとき，

$$hx'h^{-1} = f(g)f(x)f(g)^{-1} = f(gxg^{-1}) \in f(N)$$

となる．ゆえに，$gf(N)g^{-1} \subset f(N)$ となるので，$f(N)$ は H の正規部分群である．

一方，$f : G \to H$ と自然な全射準同型 $\pi : H \to H/f(N)$ との合成写像を $f' : G \to h/f(N)$ とおくと，f' は全射準同型写像である．すると，$\mathrm{Ker}(f') = N$ である．実際，$N \subset \mathrm{Ker}(f')$ であることは f' の定義から明らか．任意の $x \in \mathrm{Ker}(f')$ に対して，$f'(x) = \pi(f(x)) = (f(x))f(N)$ であるから，$(f(x))f(N) = f(N)$ となる．すなわち，$f(x) \in f(N)$ である．よって，ある $n \in N$ が存在して，$f(x) = f(n)$ となるが，f は単射ゆえ，$x = n \in N$ を得る．したがって，$\mathrm{Ker}(f') \subset N$ であることもわかる．よって，準同型定理より $G/N \cong H/f(N)$ となり，両者の位数を比較すれば求める等式を得る．

(4) $f' : G' \to H'$ を同型写像とする．このとき，写像 $f \times f' : G \times G' \to H \times H'$ を

$$(g, g') \mapsto (f(g), f(g'))$$

によって定める．すると，$f \times f'$ は同型写像である．実際，任意の $(h, h') \in H \times H'$ に対して，$h \in H$ かつ $h' \in H'$ であり，f, f' の全射性から，ある $g \in G$, $g \in G'$ が存在して $h = f(g)$, $h' = f'(g')$ となる．このとき，

$$(h, h') = (f(g), f'(g')) = (f \times f')((g, g'))$$

となるので，$f \times f'$ は全射．また，$(g_1, g_1'), (g_2, g_2') \in G \times G'$ に対して，

$$
\begin{aligned}
(f\times f')(g_1,g_1')=(f\times f')(g_2,g_2') &\iff (f(g_1),f'(g_1')) \\
&\qquad = (f(g_2),f'(g_2')) \\
&\iff f(g_1)=f(g_2) \text{ かつ } \\
&\qquad f'(g_1')=f'(g_2') \\
&\iff g_1=g_2 \text{ かつ } g_1'=g_2' \\
&\iff (g_1,g_1')=(g_2,g_2')
\end{aligned}
$$

より，$f\times f'$ は単射である．

一方，任意の $(g_1,g_1'),(g_2,g_2')\in G\times G'$ に対して，

$$
\begin{aligned}
(f\times f')((g_1,g_1')(g_2,g_2')) &= (f\times f')((g_1g_2,g_1'g_2')) \\
&= (f(g_1g_2),f'(g_1'g_2')) \\
&= (f(g_1)f(g_2),f'(g_1')f'(g_2')) \\
&= (f(g_1),f'(g_1'))(f(g_2),f'(g_2')) \\
&= (f\times f')((g_1,g_1'))(f\times f')((g_2,g_2'))
\end{aligned}
$$

となるので，$f\times f'$ は準同型写像である．よって，$f\times f'$ は同型写像である．□

一般に，群の同型類を決定する問題を考える上で，“本質的”に異なるような群の不変量をたくさん持っているとよい．というのは，与えられた二つの群 G, H が同型かどうかを判定しようとする際に，既存のいくつかの不変量を考えてみて，それらのうちのただの一つでも異なるようなものがあれば両者は同型ではないことになる．一方で，これまでに知られているどの不変量を考察しても両者を区別できない（不変量の値が一致する場合）場合は，それらは同型である可能性がより強まり，結果として同型であることが何らかの方法で証明できることがある．この，“より強まる”というところが重要で，そもそも，何の裏付けもなしに証明できるかどうかもよく分からないものを証明しようとするのは，いささかも気が進まない．というのは，証明できればよいができなかった場合はそれなりに時間とエネルギーを浪費することになる．こういう経験も大事ではあるが，数学者といえども時間は有限なので，ある程度の計算結果や予備考察に基づいた研究に着手したいと思うのが人情である．

例 3.29 位数が 6 の群 $\mathbb{Z}/6\mathbb{Z}$，および $\mathfrak{S}_3$ を考える．前者はアーベル群であり，後者は非可換群であるから，$\mathbb{Z}/6\mathbb{Z} \not\cong \mathfrak{S}_3$ である．

3.4 有限アーベル群の構造定理

この節では，これまでに解説した巡回群，直積群の概念を用いて，有限アーベル群（有限群であってアーベル群である群）の構造を完全に分類すること，すなわち，有限アーベル群の同型類を完全に決定することを考える．このような事実は，有限群アーベル群のみならず有限生成なアーベル群（さらには，単項イデアル整域上の有限生成加群）に対しても一般化されることが知られているが，本書では特に有限群に着目する関係上割愛した．興味ある読者は他の文献[35)]等を参照してほしい．

35) 例えば，松坂和夫著『代数系入門』[8] を参照せよ．

以下，単に有限アーベル群といえば，特に断らない限り乗法的有限アーベル群を考えることにする．まずは加法的巡回群 $\mathbb{Z}/n\mathbb{Z}$ の性質について考察する．

定理 3.30（中国式剰余定理（孫子の定理）） $m, n > 1$ を自然数とし，$\gcd(m, n) = 1$ とする．このとき，

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

が成り立つ．

証明. 写像 $f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ を

$$[x]_{mn} \mapsto ([x]_m, [x]_n)$$

によって定める．まず，f は well-defined である．実際，$[x]_{mn} = [y]_{mn}$ とすると，$mn|(x-y)$ となる．したがって，$m|(x-y)$ かつ $n|(x-y)$ であるから，$[x]_m = [y]_m$ かつ $[x]_n = [y]_n$ となり，$f([x]_{mn}) = f([y]_{mn})$ であることが分かる．

次に，f が準同型写像であることは，任意の $[x]_{mn}, [y]_{mn} \in \mathbb{Z}/mn\mathbb{Z}$ に対して，

$$
\begin{aligned}
f([x]_{mn}+[y]_{mn}) &= f([x+y]_{mn}) = ([x+y]_m, [x+y]_n) \\
&= ([x]_m+[y]_m, [x]_n+[y]_n) \\
&= ([x]_m, [x]_n) + ([y]_m, [y]_n) \\
&= f([x]_{mn}) + f([y]_{mn})
\end{aligned}
$$

が成り立つことから従う．

f が全単射であることを示そう．任意の $([x]_m, [y]_n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ をとる．今，$\gcd(m,n) = 1$ ゆえ，ある整数 $p, q \in \mathbb{Z}$ で $mp + nq = 1$ なるものが存在する．この両辺に x を乗じて $mxp + nxq = x$ を得る．同様に y を乗じれば $myp + nyq = y$ となる．そこで $z = myp + nxq \in \mathbb{Z}$ とおくと，

$$
[z]_m = [nxq]_m = [x]_m, \quad [z]_n = [myp]_n = [y]_n
$$

となるので，$f([z]_{mn}) = ([x]_m, [y]_n)$ を得る．よって，f は全射．一方，$[x]_{mn}, [y]_{mn} \in \mathbb{Z}/mn\mathbb{Z}$ に対して，$f([x]_{mn}) = f([y]_{mn})$ と仮定すると，$[x]_m = [y]_m$ かつ $[x]_n = [y]_n$ より，$m|(x-y)$ かつ $n|(x-y)$ を得る．ところが，$\gcd(m,n) = 1$ であるから，$mn|(x-y)$ でなければならない．すなわち，$[x-y]_{mn} = 0$ より，$[x]_{mn} = [y]_{mn}$ を得る．よって，f は単射である．□

注意 3.31 $m, n > 1$ を自然数とし，$\gcd(m,n) = 1$ とする．任意の同型写像 $f : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/mn\mathbb{Z}$ に対して

$$
\begin{aligned}
H_m &:= \{ f(([x]_m, 0)) \in \mathbb{Z}/mn\mathbb{Z} \mid [x]_m \in \mathbb{Z}/m\mathbb{Z} \}, \\
H_n &:= \{ f((0, [y]_n)) \in \mathbb{Z}/mn\mathbb{Z} \mid [y]_n \in \mathbb{Z}/n\mathbb{Z} \}
\end{aligned}
$$

とおくと，$H_m \cong \mathbb{Z}/m\mathbb{Z}$ かつ $H_n \cong \mathbb{Z}/n\mathbb{Z}$ であり，定理 3.30 より，$\mathbb{Z}/mn\mathbb{Z} = H_m \dot{\times} H_n$ となることが分かる．

このような H_m, H_n は同型写像 f の取り方によらず一意的に定まる．実際，H_m は巡回群 $\mathbb{Z}/mn\mathbb{Z}$ の位数 m の部分群であるが，命題 2.40 より，このような部分群はただ一つしかない．同様に，H_n の一意性についても分かる．

系 3.32 $n > 1$ を自然数とし，$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ を n の素因数分解

とする．ここで，$p_1 < p_2 < \cdots < p_r$ は相異なる素数であり，$e_i > 1$ とする．このとき，

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \mathbb{Z}/p_2^{e_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$$

が成り立つ．

証明． $r \geq 1$ に関する帰納法による．$r = 1$ のときは自明である．$r > 1$ とし，$r-1$ 以下の場合に主張が成り立つと仮定する．$m = p_1^{e_1}p_2^{e_2}\cdots p_{r-1}^{e_{r-1}}$ とおくと，$(m, p_r^{e_r}) = 1$ であるから，定理 3.30 より，

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$$

となる．一方，帰納法の仮定より，$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \mathbb{Z}/p_2^{e_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_{r-1}^{e_{r-1}}\mathbb{Z}$ であるから，

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \mathbb{Z}/p_2^{e_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_{r-1}^{e_{r-1}}\mathbb{Z}) \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$$

を得る．後は補題 3.22 と同様の議論によって求める結果を得る．□

注意 3.33 系 3.32 の状況の下，$\mathbb{Z}/n\mathbb{Z}$ には位数が $p_i^{e_i}$ となる部分群 $H_{p_i^{e_i}}$ が一意的に存在して，$\mathbb{Z}/n\mathbb{Z} = H_{p_1^{e_1}} \dot{\times} \cdots \dot{\times} H_{p_r^{e_r}}$ となる．

補題 3.34 $p > 1$ を素数とし，$e \geq 1$ を自然数とする．このとき，$\mathbb{Z}/p^e\mathbb{Z}$ は非自明な二つの巡回群の直積と同型にはならない．すなわち，自然数 $m, n \in \mathbb{N}$ に対して，

$$\mathbb{Z}/p^e\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \implies n = 1 \text{ または } m = 1$$

が成り立つ．

証明． $m, n > 1$ に対して，同型写像 $f : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p^e\mathbb{Z}$ が存在したとする．

$$K_m := \{([x]_m, [0]_n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \mid [x]_m \in \mathbb{Z}/m\mathbb{Z}\},$$
$$K_n := \{([0]_m, [y]_n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \mid [y]_n \in \mathbb{Z}/n\mathbb{Z}\}$$

とおくと，$K_m \cong \mathbb{Z}/m\mathbb{Z}$，$K_n \cong \mathbb{Z}/n\mathbb{Z}$ である．このとき，$f(K_m)$，$f(K_n)$ はそれぞれ，$\mathbb{Z}/p^e\mathbb{Z}$ の位数 m，n の部分群であるから，m と

n は p^e の約数，すなわち p の冪乗[36] の形をしている．したがって，$p|m$ かつ $p|n$ となり，命題 2.40 より，$\mathbb{Z}/m\mathbb{Z}$ と $\mathbb{Z}/n\mathbb{Z}$ には位数 p の部分群がそれぞれ一意的に存在する．よって，$f(K_m)$, $f(K_n)$ にも位数 p の部分群が存在することが分かる．これらをそれぞれ A, B とおと，$A \neq B$ である．実際，$A = B$ とする．位数 p の群は巡回群ゆえ，$A = B = \langle a \rangle$ なる $a \in A = B$ が存在する．すると，

$$f^{-1}(a) \in f^{-1}(A) \cap f^{-1}(B) \subset K_m \cap K_n = \{(0,0)\}$$

であるから，$a = (0,0)$ でなければならない．これは矛盾である．よって，$A \neq B$.

ところが，巡回群 $\to \mathbb{Z}/p^e\mathbb{Z}$ において，位数が p の部分群は一意的であるからやはり矛盾．したがって，$f : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p^e\mathbb{Z}$ なる同型写像は存在しない．□

36) “べき” を表す漢字は “冪” の他に，略字である “巾” も用いられることがある．

注意 3.35 補題 3.34 を内部直積を用いていい換えると，

「$\mathbb{Z}/p^e\mathbb{Z}$ は真部分群の内部直積として表すことはできない．」

となる．一般に，群 G が部分群 H と K に対して，$G = H \dot{\times} K$ ならば $H = \{1\}$ または $K = \{1\}$ を満たすとき，G は**直既約** (direct indecomposable) であるという．上の議論から，位数が素数冪の巡回群は直既約であることが分かる．

補題 3.36 G を乗法的有限アーベル群とし，G に含まれる元の位数の最大値を m とする．このとき，任意の $g \in G$ に対して，g の位数は m の約数で，$g^m = 1_G$ である．

証明. $|G|$ の相異なる素因数を $p_1, p_2, \ldots, p_r$ とする．各 $1 \leq i \leq r$ に対して，G の元であって，位数が p_i の冪乗となるもののうち最大のものを $x_i \in G$ とおく．x_i の位数を $p_i^{e_i}$ $(e_i \geq 0)$ とする．このとき，$x := x_1 x_2 \cdots x_r$ とおくと，補題 2.39 を帰納的に用いることにより，x の位数は $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ であることが分かる．

さて，任意の $g \in G$ に対して，g の位数 n は G の位数の約数であるから，n は $n = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$ $(f_i \geq 0)$ なる形に書けることが分かる．系 3.32 より，位数 n の巡回群 $\langle g \rangle$ は，位数 $p_i^{f_i}$ の部分

群 $H_{p_i^{f_i}}$ たちの内部直積となる．つまり，g_i を $H_{p_i^{f_i}}$ の生成元とすれば，$g = g_1 g_2 \cdots g_r$ となる．今，x_i の定義における位数の最大性から，各 $1 \leq i \leq r$ に対して，$p_i^{f_i} \leq p_i^{e_i}$ となっている．ゆえに，$n = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r} \leq p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ を得る．すなわち，G の任意の元の位数は $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ を超えない．これは，$m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ であることを示している．したがって，任意の元 $g \in G$ の位数は m の約数であり，$g^m = 1_G$ となることが分かる．□

補題 3.37 G を乗法的有限アーベル群，x を位数が最大となる G の元とする．このとき，$H := \langle x \rangle$ とおくと，$G = H \dot{\times} K$ となる G の部分群 K が存在する．

証明. $|G|$ に関する帰納法による．G が自明な群 $E := \{1_G\}$ に等しいときは，$G = E \dot{\times} E$ となるので明らか．次に，$|G| = 2$ の場合を考える．より一般に，$|G|$ が素数 p の場合を考えよう．このとき，G は位数 p の巡回群であるから $G = \langle x \rangle$ と書ける．このとき，$H = \langle x \rangle$ であり，$G = H \dot{\times} E$ となる．そこで，以下，$|G| \geq 3$ とする．

$G = H$ の場合は，$K = E$ とすれは上と同様の議論により題意が示される．そこで，$G \neq H$ と仮定する．G はアーベル群なので H は G の正規部分群であり，その剰余群 G/H が考えられる．仮定 $G \neq H$ より，G/H は非自明な群であるから，ある $yH \in G/H$ で $yH \neq H$ なるものが存在する．G/H において yH が生成する部分群 $\langle yH \rangle$ を考える．$yH \neq H$ より，yH の G/H における位数は 2 以上である．p を yH の位数の素因数のうちの一つとすると，$|\langle yH \rangle|$ は p の倍数となるので，命題 2.40 より，$\langle yH \rangle$ は位数 p の巡回群 $P = \langle zH \rangle$ をただ一つ部分群として含む．このとき，$z \notin H$，$z^p \in H$ であるから，ある $s \in \mathbb{N}$ が存在して $z^p = x^s$ となる．x の位数を m とすると，補題 3.36 より，z の位数 l は m の約数である．また，$(zH)^l = z^l H = H \in G/H$ であり，zH の G/H における位数は p であるから，l は p の倍数である．よって，m は p の倍数であることが分かる．すると，

$$x^{s\frac{m}{p}} = z^{p\frac{m}{p}} = z^m = 1_G$$

であるから，$s\frac{m}{p}$ は m の倍数であることが分かり，これより，s が

pの倍数であることが分かる．

さて，$x_1 = x^{\frac{s}{p}}$ とすると，$x_1 \in H$ かつ $z^p = x^s = x_1^p$ となる．よって，$w = zx_1^{-1}$ とおくと，$w^p = 1_G$ であり $w \notin H$ である．実際，$w \in H$ とすると $z = wx_1 \in H$ となって矛盾．そこで，$P = \langle w \rangle$ とおくと，P は位数 p の非自明な群なので巡回群である．このとき，$P \cap H$ は P の部分群であるが，位数 p の巡回群の部分群は自明な群か自分自身のどちらかしかない．$P \cap H = P$ と仮定すると，$P \subset H$ となり $w \notin H$ に矛盾する．よって，$P \cap H = \{1_G\}$ である．

次に，$\overline{G} := G/P$, $\overline{H} := HP/P$ なる群を考える．注意 3.18 により，$\overline{H} \leq \overline{G}$ とみなす．いま，$\overline{H} = \langle xP \rangle$ である．実際，任意の $\alpha\beta P \in \overline{H}$, $(\alpha \in H,\ \beta \in P)$ に対して，$\alpha\beta P = \alpha P \in \overline{H}$ であり，$\alpha \in H$ より $\alpha = x^u$ なる $u \in \mathbb{Z}$ が存在する．よって，$\alpha\beta P = (xP)^u \in \langle xP \rangle$ となり，$\overline{H} \subset \langle xP \rangle$ を得る．逆の包含関係は明らか．また，第二同型定理を用いて

$$\overline{H} = HP/P \cong H/(H \cap P) = H/\{1_G\} = H$$

が成り立つ．一方，$\overline{G}$ において位数最大の元は xP である．実際，$\overline{H} \cong H$ なので，xP の位数は x の位数 m に等しい．任意の $\gamma P \in \overline{G}$ に対して，$\gamma \in G$ の位数を k とすると，$(\gamma P)^k = \gamma^k P = P$ となるので γP の位数 k' は k の約数である．つまり k 以下である．一方，x の定義から $k \leq m$ であるから，結局，$k' \leq m$ を得る．よって，xP は $\overline{G}$ における位数最大の元である．

ここで，帰納法の仮定を用いることで，$\overline{G}$ には，$\overline{G} = \overline{H} \dot{\times} \overline{K}$ となる部分群 $\overline{K}$ が存在することが分かる．特に，対応原理および，注意 3.18 を考慮すると，P を含むような G のある部分群 K が存在して $\overline{K} = K/P$ と書けることが分かる．さらに，

$$(H \cap K)P/P \subset \overline{H} \cap \overline{K} = \{1_{G/P}\}$$

であるから，$H \cap K \subset P$ となる．ところが，P は位数 p の巡回群ゆえ，これは $H \cap K = \{1_G\}$ または，$H \cap K = P$ を意味する．もし，$H \cap K = P$ となったとすると，$P \subset H$ となるのでこれは上述の議論に矛盾する．よって，$H \cap K = \{1_G\}$．したがって，定理 3.25 より，$HK = H \dot{\times} K$ である．特に，$H \dot{\times} K \subset G$ であり，

$$|G| = |G/P|\,|P| = |\overline{G}|\,|P| = |\overline{H}|\,|\overline{K}|\,|P| = |H|\,|\overline{K}|\,|P| = |H|\,|K|$$

となるので，$G = H \dot{\times} K$ であることが分かる．よって帰納法が進む．
□

一般に，乗法群 G および，任意の $k \geq 1$ に対して，G の k 個の積を $G^k := GG \cdots G \leq G$ と書く．

補題 3.38 G を群とし，$G = H_{e_1} \dot{\times} H_{e_2} \dot{\times} \cdots \dot{\times} H_{e_m}$ とする．このとき，

$$G^k = H_{e_1}^k \dot{\times} H_{e_2}^k \dot{\times} \cdots \dot{\times} H_{e_m}^k$$

が成り立つ．

証明. まず，$G^k = H_{e_1}^k H_{e_2}^k \cdots H_{e_m}^k$ となることを示そう．$\supset$ は明らかゆえ，$\subset$ を示す．任意の $g \in G^k$ に対して，$g = g_1 g_2 \cdots g_k$ なる $g_i \in G$ がとれる．さらに, 各 $1 \leq i \leq k$ に対して, $g_i = h_{i1} h_{i2} \cdots h_{im}$ なる元 $h_{ij} \in H_j$ がとれる．このとき，H_i の各元と H_j の各元は交換可能であるから，

$$\begin{aligned} g^k &= (h_{11} h_{12} \cdots h_{1m})(h_{21} h_{22} \cdots h_{2m}) \cdots (h_{k1} h_{k2} \cdots h_{km}) \\ &= (h_{11} h_{21} \cdots h_{k1})(h_{12} h_{22} \cdots h_{k2}) \cdots (h_{1m} h_{2m} \cdots h_{km}) \in \text{右辺} \end{aligned}$$

を得る．

次に，上の議論により，G^k の各元は $h_1' h_2' \cdots h_m'$, $(h_i' \in H_i^k)$ という形に表すことができる．ところが，各 $1 \leq i \leq m$ に対して，$H_i^k \leq H_i$ であるから，G 自身の内部直積の表示の一意性より，$h_1' h_2' \cdots h_m'$ のような表し方は一意的でなければならない．一方，任意の $1 \leq i, j \leq m$ に対して，H_i^k の各元と H_j^k の各元の可換性についても，H_i と H_j についてのそれから直ちに得られる．ゆえに，求める $G = H_{e_1}^k \dot{\times} H_{e_2}^k \dot{\times} \cdots \dot{\times} H_{e_m}^k$ である．□

定理 3.39（有限アーベル群の構造定理） G を単位群ではない乗法的有限アーベル群とする．このとき，G は以下のような巡回群たちの内部直積になる：

$$G = H_{e_1} \dot{\times} H_{e_2} \dot{\times} \cdots \dot{\times} H_{e_m}.$$

ここで，各 e_i たちは

$$e_i > 1\ (1 \le i \le m), \quad e_i | e_{i-1}\ (2 \le i \le m)$$

を満たし，H_{e_i} は G の部分群で，位数 e_i の巡回群である．このような H_{e_i} たちは G に対して一意的に定まる．

一方，上の状況において

$$G \cong \mathbb{Z}/e_1\mathbb{Z} \times \mathbb{Z}/e_2\mathbb{Z} \times \cdots \times \mathbb{Z}/e_m\mathbb{Z}$$

であるが，このような e_i たちの組 $(e_1, e_2, \ldots, e_m)$ は G の同型を除いて一意的に定まる．

証明． まず，G を単位群ではない有限アーベル群とするとき，G が題意のような巡回群の内部直積として表せることを示そう．そこで，x_1 を G の位数最大の元とし，その位数を e_1 とする．このとき，$H_{e_1} := \langle x_1 \rangle$ とおくと，H_{e_1} は位数 e_1 の巡回群であり，補題 3.37 により，$G = H_{e_1} \dot{\times} K_1$ なる G の部分群 K_1 が存在する．K_1 が自明な群であれば，$G = H_{e_1} \cong \mathbb{Z}/e_1\mathbb{Z}$ となる．もし，K_1 が自明な群でなければ，x_2 を K_1 の中の位数最大の元とし，その位数を e_2 とする．すると，$H_{e_2} := \langle x_2 \rangle$ とおけば同様の議論から，$H_{e_2} \cong \mathbb{Z}/e_2\mathbb{Z}$ かつ，$K_1 = H_{e_2} \dot{\times} K_2$ なる K_1 の部分群 K_2 が存在する．また，補題 3.36 より，e_2 は e_1 の約数である．以下，同様の議論を繰り返すことにより，G は有限群であるからいつかは

$$G = H_{e_1} \dot{\times} H_{e_2} \dot{\times} \cdots \dot{\times} H_{e_m}, \quad e_m | e_{m-1} | \cdots | e_2 | e_1$$

なる形に到達する．このとき，$G \cong \mathbb{Z}/e_1\mathbb{Z} \times \mathbb{Z}/e_2\mathbb{Z} \times \cdots \times \mathbb{Z}/e_m\mathbb{Z}$ である．

次に，表示の一意性を示そう．そこで，G が二通りの内部直積による表示

$$G = H_{e_1} \dot{\times} H_{e_2} \dot{\times} \cdots \dot{\times} H_{e_m} = K_{f_1} \dot{\times} K_{f_2} \dot{\times} \cdots \dot{\times} K_{f_n}$$

を持ったとする．ここで，$H_{e_i} = \langle x_i \rangle$，$K_{f_j} = \langle y_j \rangle$ はそれぞれ，位数 e_i，f_j の巡回群である．いま，$e_1 \neq f_1$ と仮定する．対称性から $f_1 > e_1$ としても一般性を失わない．補題 3.38 より，

$$H_{e_1}^{e_1} \dot{\times} H_{e_2}^{e_1} \dot{\times} \cdots \dot{\times} H_{e_m}^{e_1} = K_{f_1}^{e_1} \dot{\times} K_{f_2}^{e_1} \dot{\times} \cdots \dot{\times} K_{f_n}^{e_1} \tag{3.1}$$

となるが，$e_2, e_3, \ldots, e_m$ は e_1 の約数であるから，$x_i^{e_1} = 1_G$, $(2 \le i \le m)$ である．したがって，

$$\{1_G\} = K_{f_1}^{e_1} \dot{\times} K_{f_2}^{e_1} \dot{\times} \cdots \dot{\times} K_{f_n}^{e_1}$$

でなければならない．よって，両辺の位数を比較して，$K_{f_j}^{e_j} = \{1_G\}$ $(1 \le j \le n)$ でなければならないが，特に $K_{f_1}^{e_1} = \{1_G\}$ より，$y_1^{e_1} = 1_G$ でなければならない．ところが，y_1 の位数 f_1 は e_1 より真に大きいのでこれは矛盾．よって，$e_1 = f_1$ である．

さて，$e_2 \neq f_2$ と仮定する．$f_2 > e_2$ としても一般性を失わない．今，$e_3, e_4, \ldots, e_m$ は e_2 の倍数であるから，上とまったく同様の議論により，

$$H_{e_1}^{e_2} = K_{f_1}^{e_2} \dot{\times} K_{f_2}^{e_2} \dot{\times} \cdots \dot{\times} K_{f_n}^{e_2}$$

を得る．$e_1 = f_1$ に注意して両辺の位数を比較すれば，$K_{f_j}^{e_j} = \{1_G\}$, $(2 \le j \le n)$, を得る．特に，$K_{f_2}^{e_2} = \{1_G\}$ より，$y_2^{e_2} = 1_G$ となるが，これは矛盾．よって，$e_2 = f_2$.

以下同様に繰り返すことにより，逐次，$e_1 = f_1, e_2 = f_2, \ldots$ を得る．このとき，もし，$m < n$ もしくは $n < m$ となったとすると，等式 (3.1) の両辺の位数が等しくならないので矛盾．よって，$m = n$ であることも分かる．

最後に，$(e_1, e_2, \ldots, e_m)$ が G の同型を除いて一意的に定まることを示す．そこで，$\psi : G' \to G$ を有限アーベル群の同型写像とし，

$$G = H_{e_1} \dot{\times} H_{e_2} \dot{\times} \cdots \dot{\times} H_{e_m}, \quad G' = K_{f_1} \dot{\times} K_{f_2} \dot{\times} \cdots \dot{\times} K_{f_n}$$

を上で述べたことから得られる，G と G' の一意的な内部直積表示とする．このとき，ψ は同型写像であるから，G は

$$G = \psi(K_{f_1}) \dot{\times} \psi(K_{f_2}) \dot{\times} \cdots \dot{\times} \psi(K_{f_n})$$

という内部直積表示を持つ．このとき，表示の一意性から，$m = n$ かつ，各 $1 \le i \le m$ に対して $\psi(K_{f_i}) = H_{e_i}$ でなければならない．ゆえに，$e_i = f_i$ を得る．つまり，$(f_1, f_2, \ldots, f_n) = (e_1, e_2, \ldots, e_m)$

である．以上より求める結果を得る．□

定義 3.40（**単因子**）有限アーベル群 G に対して，定理 3.39 より同型を除いて一意的に定まる自然数の組 $(e_1, e_2, \ldots, e_m)$ を G の**単因子** (elementary divisor) もしくは，**不変系** (invariant system) などという．このとき，有限アーベル群 G，H に対して，

$$G \cong H \iff G \text{ と } H \text{ の単因子が一致}$$

が成り立つ．すなわち，有限アーベル群の同型類は単因子によって完全に決定できる．

一般に，定理 3.39 と並んでもう一つ有限アーベル群の構造定理と呼ばれるものがある．それを解説するために，定理 3.39 の系として得られる一つ補題を用意する．便宜的に次の記号を導入する．大きい順に並んでいる自然数の組 $(a_1, a_2, \ldots, a_m)$, $(a_1 \geq a_2 \geq \cdots \geq a_m)$ を考える．二つの組 $(a_1, a_2, \ldots, a_m)$, $(b_1, b_2, \ldots, b_n)$ に対して，これらが等しいとは，$m = n$ かつ，$a_i = b_i$, $(1 \leq i \leq m)$ が成り立つこととする．

補題 3.41 $p > 1$ を素数とする．自然数の組 $(a_1, a_2, \ldots, a_m)$, $(b_1, b_2, \ldots, b_n)$ に対して，

$$(a_1, a_2, \ldots, a_m) \neq (b_1, b_2, \ldots, b_n)$$

であれば

$$\mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_m}\mathbb{Z} \ncong \mathbb{Z}/p^{b_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{b_n}\mathbb{Z}$$

となる．

証明. 左辺の群 $\mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_m}\mathbb{Z}$ の単因子は $(p^{a_1}, p^{a_2}, \ldots, p^{a_m})$ であり, 右辺の群 $\mathbb{Z}/p^{b_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{b_n}\mathbb{Z}$ の単因子は $(p^{b_1}, p^{b_2}, \ldots, p^{b_m})$ であるから明らか．□

定理 3.42（**有限アーベル群の構造定理 その 2**）G を単位群ではない有限アーベル群とする．このとき，G は位数が素数冪であるような巡回群の直積に同型である．すなわち，

$$G \cong (\mathbb{Z}/p_1^{a_{11}}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_1^{a_{1m_1}}\mathbb{Z})\times\cdots\times(\mathbb{Z}/p_r^{a_{r1}}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_r^{a_{rm_r}}\mathbb{Z}).$$

ここで，各 p_i は $p_1 < p_2 < \cdots < p_r$ なる素数である．また，各 $a_{ij} \geq 1$ は自然数であり，各 $1 \leq i \leq m$ に対して $a_{i1} \geq a_{i2} \geq \cdots \geq a_{im_i}$ である．

さらに，このような素数冪の組 $(p_1^{a_{11}}, p_1^{a_{12}}, \ldots, p_r^{a_{rm_r}})$ は G の同型を除いて一意的に定まる．

証明． まず，任意の有限アーベル群 G に対して，定理 3.39 より，G はいくつかの巡回群の内部直積になる．したがって，巡回群の外部直積に同型である．一方，中国式剰余定理により，それらの各巡回群はさらに，位数が素数冪であるような巡回群の外部直積と同型である．よって，G が題意のような表示を持つことが分かる．

次に，この外部直積表示が同型を除いて一意的であることを示そう．そこでまず，題にある等式の右辺の群を G' とおいて，G' の単因子を求めることを考える．今，$1 \leq i \leq r$ に対して，m_i の最大値を m とおく．表記を簡単にするため，各 $1 \leq i \leq r$ に対して，必要であれば a_{1m_i} の後ろに 0 を並べることで，初めから $m_1 = m_2 = \cdots = m_r = m$ であると仮定する．このとき，各 $1 \leq j \leq m$ に対して，

$$e_j := p_1^{a_{1j}} p_2^{a_{2j}} \cdots p_r^{a_{rj}}$$

とおくと，$e_m | e_{m-1} | \cdots | e_2 | e_1$ となる．さらに，中国式剰余定理によって

$$\mathbb{Z}/e_j\mathbb{Z} \cong \mathbb{Z}/p_1^{a_{1j}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{a_{rj}}\mathbb{Z}$$

であるから，$(e_1, e_2, \ldots, e_m)$ が G' の単因子である．

さて，G が別の外部直積表示

$$G \cong (\mathbb{Z}/q_1^{b_{11}}\mathbb{Z}\times\cdots\times\mathbb{Z}/q_1^{b_{1n_1}}\mathbb{Z})\times\cdots\times(\mathbb{Z}/q_s^{b_{s1}}\mathbb{Z}\times\cdots\times\mathbb{Z}/q_s^{b_{sn_s}}\mathbb{Z})$$

を持ったとする．上式右辺の群を G'' とおく．このとき，G' と G'' の単因子は一致している．上で述べた単因子の構成（特に素因数分解）を考えると，$r = s$ であり，各 $1 \leq i \leq r$ に対して $q_i = p_i$ でなければならないことが分かる．さらに，各素数の冪指数が等しいことは以下のようにして分かる．G' の単因子を求めた時と同様に，

$n_1, n_2, \ldots, n_r$ の最大値を n として，G'' の単因子を $(e'_1, e'_2, \ldots, e'_n)$ とする．まず，$m_{i_0} = m$ なる i_0 に対し，p_{i_0} の冪指数 $a_{i_0 j}$ に注目する．$a_{i_0 1} \geq \cdots \geq a_{i_0 m} \geq 1$ である．もし，$a_{i_0 t} \neq b_{i_0 t}$ なる $1 \leq t \leq m$ が存在したとすると，素因数分解における p_{i_0} の指数を考えることで，$e_t \neq e'_t$ となり，これは矛盾．よって，$m \leq n$ かつ $a_{i_0 j} = b_{i_0 j}, (1 \leq j \leq m)$ である．G' と G'' の役割を入れ換えて考えることで，$n \leq m$ であることも分かり，したがって，$m = n$ を得る．このとき，任意の $1 \leq i \leq r$ に対して，

$$(a_{i1}, a_{i2}, \ldots, a_{i_m}) = (b_{i1}, b_{i2}, \ldots, b_{im})$$

となることが，$i = i_0$ のときの議論と同様にして分かる．以上により，素数冪の組 $(p_1^{a_{11}}, p_1^{a_{12}}, \ldots, p_r^{a_{rm_r}})$ は G の同型を除いて一意的である．□

注意 3.43 定理 3.42 における素数冪の組 $(p_1^{a_{11}}, p_1^{a_{12}}, \ldots, p_r^{a_{rm_r}})$ はあくまで G の同型を除いて一意的に定まるもので，定理 3.39 のように，G がこのような素数冪の巡回群の内部直積として一意的に分解するというわけではない．実際，$\mathbb{Z}/2\mathbb{Z} = \{0, [1]_2\}$ に対して，$G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ を考える．

$$H := \{(a, 0) \in G \mid a \in \mathbb{Z}/2\mathbb{Z}\}, \quad K := \{(0, b) \in G \mid b \in \mathbb{Z}/2\mathbb{Z}\}$$

とおくと，$G = H \dot{\times} K$ であるが，

$$L := \{(c, c) \in G \mid c \in \mathbb{Z}/2\mathbb{Z}\}$$

なる部分群を考えても，$G = H \dot{\times} L = K \dot{\times} L$ となる．

この節の最後に，有限アーベル群の部分群に関する以下の定理を述べる．シローの定理の特別な場合とみなせる．

定理 3.44 G を単位群ではない乗法的有限アーベル群とし，$|G|$ の素因数分解を

$$|G| = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, \quad p_1 < p_2 < \cdots < p_r$$

とする．このとき，各 $1 \leq i \leq r$ に対して，G は位数 $p_i^{e_i}$ の部分群

をただ一つ持つ．この群を P_i とおくと P_i は，位数が p_i の冪になるような G の元全体からなる G の部分群である．

さらに，$G = P_1 \dot{\times} P_2 \dot{\times} \cdots \dot{\times} P_r$ であり，このような分解は G に対して一意的である．

証明. G の元で，位数が p_i の冪乗となるような元全体の集合を P'_i とおく．すると，$1_G = p_i^0 \in P'_i$ であり，任意の $x, y \in P'_i$ に対して，xy および x^{-1} の位数は p_i の冪である．実際，x, y の位数をそれぞれ p_i^a, p_i^b とすると，xy, x^{-1} の位数は $p_i^{\max(a,b)}$, p_i^a である．したがって，P'_i は G の部分群である．

このとき，G における部分群の積 $P'_1 P'_2 \cdots P'_r$ は内部直積 $P'_1 \dot{\times} P'_2 \dot{\times} \cdots \dot{\times} P'_r$ である．実際，任意の $1 \leq i \leq r-1$ に対して，$P'_1 \cdots P'_i$ に含まれる元の位数は $p_1^{a_1} \cdots p_i^{a_i}$ なる形をしており，P'_{i+1} に含まれる元の位数は $p_{i+1}^{a_{i+1}}$ なる形をしているから，$(P'_1 \cdots P'_i) \cap P'_{i+1} = \{1_G\}$ である．よって，定理 3.25 より $P'_1 P'_2 \cdots P'_r = P'_1 \dot{\times} P'_2 \dot{\times} \cdots \dot{\times} P'_r \subset G$ である．一方，任意の $g \in G$ に対して，定理 3.42 より g は $g = x_1 x_2 \cdots x_r$ $(x_i \in P'_i)$ と書ける．ゆえに，$G = P'_1 \dot{\times} P'_2 \dot{\times} \cdots \dot{\times} P'_r$ である．各 P'_i の位数は p_i の冪乗の形をしているが，$p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} = |P'_1||P'_2| \cdots |P'_r|$ であるから，$|P'_i| = p_i^{e_i}$ でなければならない．したがって，$P'_i = P_i$ である．P_i の一意性については構成から明らかである．□

3.5 群のアーベル化

与えられた群がどのような構造を有するのかを調べようとする際，その群のみに注目していると難しすぎて手が出ないことがしばしばある（というか，ほとんど手が出ない）．そこで，まずは元の群をより簡単な群で近似できないかということを考える．その一例が群のアーベル化である．率直にいえば，与えられた群に最も構造的に“近い”アーベル群は何かを決定する問題である．アーベル化を決定しただけで元の群の構造がいつもよく分かるなどというほど世の中そう甘くはないが，アーベル化はいわゆる群の不変量でもあり，簡易的な応用例として，「与えられた二つの群そのものはよく分からない

が，両者のアーベル化を見るとアーベル群として同型ではないので，元々の群は同型ではない」などの利用法がある．

定義 3.45（**交換子群**）G を群とする．任意の元 $x,y\in G$ に対して，$[x,y]:=xyx^{-1}y^{-1}$ を x と y の**交換子** (commutator) という．G 内の交換子すべてで生成される部分群

$$[G,G]:=\langle\, [x,y]\in G\,|\, x,y\in G\rangle\leq G$$

を G の**交換子群** (commutator subgroup) [37] という．

[37] 日本語で交換子部分群といういい方はあまり聞いたことがない．

補題 3.46 G を群とする．

(1) 任意の $x,y\in G$ に対して，$[x,y]^{-1}=[y,x]$ が成り立つ．したがって，$[G,G]$ の各元は，

$$[x_1,y_1][x_2,y_2]\cdots[x_m,y_m]$$

のように，G の交換子たちの有限積で表すことができる．

(2) 任意の $x,y,z\in G$ に対して，

$$z[x,y]z^{-1}=[zxz^{-1},zyz^{-1}]$$

が成り立つ．

(3) $[G,G]\lhd G$．すなわち，交換子群は正規部分群である．

(4) 任意の準同型写像 $f:G\to H$ に対して，$f([G,G])\subset[H,H]$．

証明．(1) 任意の $x,y\in G$ に対して，

$$[x,y][y,x]=(xyx^{-1}y^{-1})(yxy^{-1}x^{-1})=1_G$$

である．$[y,x][x,y]=1_G$ も同様である．したがって，$[x,y]^{-1}=[y,x]$．この事実より，後半の主張は明らか．

(2) 具体的に計算すればよい．実際，

$$\begin{aligned}z[x,y]z^{-1}&=z(xyx^{-1}y^{-1})z^{-1}\\&=(zxz^{-1})(zyz^{-1})(zx^{-1}z^{-1})(zy^{-1}z^{-1})\\&=[zxz^{-1},zyz^{-1}]\end{aligned}$$

である．

(3) 任意の $z \in [G,G]$ と任意の $g \in G$ をとる．$z = [x_1,y_1][x_2,y_2]\cdots[x_m,y_m]$ $(x_i,y_i \in G)$ とするとき，

$$\begin{aligned}
gzg^{-1} &= g[x_1,y_1][x_2,y_2]\cdots[x_m,y_m]g^{-1} \\
&= (g[x_1,y_1]g^{-1})(g[x_2,y_2]g^{-1})\cdots(g[x_m,y_m]g^{-1}) \\
&= [gx_1g^{-1},gy_1g^{-1}][gx_2g^{-1},gy_2g^{-1}]\cdots \\
&\qquad\qquad \cdots[gx_mg^{-1},gy_mg^{-1}] \in [G,G]
\end{aligned}$$

となる．ゆえに，$g[G,G]g^{-1} \subset [G,G]$ を得る．

(4) 任意の交換子 $[x,y] \in [G,G]$ に対して，f は準同型写像であるから $f([x,y]) = [f(x),f(y)] \in H$ となる．$[G,G]$ は交換子たちで生成されるので，$f([G,G]) \subset [H,H]$ である．□

補題 3.47 G をアーベル群とするとき，$[G,G]$ は自明な群 $\{1_G\}$ に一致する．

証明． 任意の交換子 $[x,y] \in G$ に対して，G はアーベル群であるから，$[x,y] = xyx^{-1}y^{-1} = xx^{-1}yy^{-1} = 1_G$ となる．$[G,G]$ は交換子たちで生成されるので，$[G,G] = \{1_G\}$ である．□

定義 3.48 G を群とする．G の交換子群 $[G,G]$ による剰余群 $G/[G,G]$ を，G の**アーベル化** (abelianization) といい，G^{ab} と表す．

任意の群 G に対して G^{ab} はアーベル群である．実際，G^{ab} の任意の交換子 $[x[G,G],y[G,G]]$ は，$[x[G,G],y[G,G]] = [x,y][G,G] = [G,G]$ であるから，単位元に等しい．よって，$[G^{\mathrm{ab}},G^{\mathrm{ab}}] = \{[G,G]\} = \{1_{G^{\mathrm{ab}}}\}$ を得る．

補題 3.49 G，H を群とし，$G \cong H$ する．このとき，$G^{\mathrm{ab}} \cong H^{\mathrm{ab}}$．

証明． $f : G \to H$ を同型写像とする．f と自然な全射準同型 $\pi : H \to H^{\mathrm{ab}}$ の合成写像を $f' : G \to H^{\mathrm{ab}}$ とおく．f' は全射準同型写像である．このとき，$\mathrm{Ker}(f') = [G,G]$ である．実際，任意の $g \in \mathrm{Ker}(f')$ に対して，$f'(g) = f(g)[H,H] = [H,H]$ であるから，H のある交換子 $h_1,\ldots,h_t \in [H,H]$ が存在して，$f(g) = h_1h_2\cdots h_t$

と書ける．このとき，$g = f^{-1}(h_1)f^{-1}(h_2)\cdots f^{-1}(h_t)$ であり，f^{-1} は準同型写像であるから各 $1 \leq i \leq t$ に対して $f^{-1}(h_i) \in [G,G]$ である．ゆえに，$g \in [G,G]$ となる．逆に，$g \in [G,G]$ であれば，$g \in \mathrm{Ker}(f')$ であることは明らか．よって，準同型定理から求める結果を得る．□

定理 3.50 G を群とし，$\pi : G \to G^{\mathrm{ab}}$ を自然な全射準同型写像とする．A をアーベル群とし，任意の準同型写像 $f : G \to A$ を考える．

(1) $[G,G] \subset \mathrm{Ker}(f)$.
(2) ある準同型写像 $\overline{f} : G^{\mathrm{ab}} \to A$ が一意的に存在して，$f = \overline{f} \circ \pi$ となる．

証明. (1) 任意の交換子 $[x,y] \in [G,G]$ に対して，f は準同型写像であり，A はアーベル群であるから $f([x,y]) = [f(x), f(y)] = 1_A$ となる．$[G,G]$ は交換子で生成されるので求める結果を得る．

(2) (1) と補題 3.10 により，f は準同型写像 $\overline{f} : G^{\mathrm{ab}} \to A$, $g[G,G] \mapsto f(g)$ を誘導する．このとき，$f = \overline{f} \circ \pi$ である．一意性については，$F : G^{\mathrm{ab}} \to A$ も準同型写像で，$f = F \circ \pi$ を満たしたとすると，任意の $g[G,G] \in G^{\mathrm{ab}}$ に対して

$$F(g[G,G]) = f(g) = \overline{f}(g[G,G])$$

となるので明らか．□

注意 3.51 定理 3.50 の (1) より，$[G,G]$ は，剰余群がアーベル群となるような G の正規部分群の中で最小のものであることが分かる．また，(2) より，G のアーベル化は G の剰余群でアーベル群であるもののうち，"最大のもの" であることも分かる．この意味で，G^{ab} を G の**最大アーベル商** (maximal abelian quotient) ともいう．

例 3.52（対称群のアーベル化） 自然数 $n \geq 2$，および n 次対称群 $\mathfrak{S}_n$ に対して，

$$[\mathfrak{S}_n, \mathfrak{S}_n] = \begin{cases} \{1_{\mathfrak{S}_n}\}, & n = 2 \\ \mathfrak{A}_n, & n \geq 3 \end{cases}$$

となる．実際，$n=2$ のとき $\mathfrak{S}_2$ はアーベル群だから，$[\mathfrak{S}_2, \mathfrak{S}_2] = \{1_{\mathfrak{S}_2}\}$．以下，$n \geq 3$ とする．今，$\mathfrak{A}_n = \mathrm{Ker(sgn)}$ であり，sgn の像 $\{\pm 1\}$ はアーベル群であるので，定理 3.50 より，$[\mathfrak{S}_n, \mathfrak{S}_n] \subset \mathrm{Ker(sgn)} = \mathfrak{A}_n$ となる．一方，$\mathfrak{A}_n$ は $(1\,2\,k)$ $(k \geq 3)$ という形の元で生成されるが，

$$(1\,2\,k) = (1\,2)(1\,2\,k)(1\,2)^{-1}(1\,2\,k)^{-1} \in [\mathfrak{S}_n, \mathfrak{S}_n]$$

であるから $\mathfrak{A}_n \subset [\mathfrak{S}_n, \mathfrak{S}_n]$ となる．よって，$\mathfrak{A}_n = [\mathfrak{S}_n, \mathfrak{S}_n]$ を得る．

以上より，任意の $n \geq 2$ に対して

$$\mathfrak{S}_n^{\mathrm{ab}} = \mathfrak{S}_n/\mathfrak{A}_n \cong \mathbb{Z}/2\mathbb{Z}$$

であることが分かる．実際，$n=2$ のときは $\mathfrak{A}_2 = \{1_{\mathfrak{S}_1}\}$ だから明らかであり，$n \geq 3$ のときは，符号関数 $\mathrm{sgn} : \mathfrak{S}_n \to \{\pm 1\}$ に準同型定理を適用すればよい．

例 3.53（交代群のアーベル化） $n=2$ のとき，明らかに $\mathfrak{A}_2 = \{1_{\mathfrak{A}_2}\}$ であるから，$\mathfrak{A}_2^{\mathrm{ab}} \cong \{1_{\mathfrak{A}_2^{\mathrm{ab}}}\}$．また，$n=3$ のとき，

$$\mathfrak{A}_3 = \{1_{\mathfrak{A}_3},\ (123),\ (132)\}$$

である．すなわち，$\mathfrak{A}_3$ はアーベル群である．よって，$\mathfrak{A}_3^{\mathrm{ab}} = \mathfrak{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$ である．$n=4$ のときは例 4.19 を参照せよ．

自然数 $n \geq 5$ に対して，$[\mathfrak{A}_n, \mathfrak{A}_n] = \mathfrak{A}_n$ となる．これを示すには $\supset$ の包含関係を示せばよい．逆は明らかである．$\mathfrak{A}_n$ は $(1\,2\,k)$ $(k \geq 3)$ なる形の元で生成される．$n \geq 5$ より，$i \neq j$ なる i, j であって，$i, j \neq 1, 2, k$ となるものが存在する．このとき，

$$(1\,2\,k) = (1\,2\,i)(1\,2\,i\,k\,j)(1\,2\,i)^{-1}(1\,2\,i\,k\,j)^{-1} \in [\mathfrak{A}_n, \mathfrak{A}_n]$$

となるので，$\mathfrak{A}_n \subset [\mathfrak{A}_n, \mathfrak{A}_n]$ となる．よって，求める等式を得る．

すなわち，$n \geq 5$ のとき，

$$\mathfrak{A}_n^{\mathrm{ab}} \cong \{1_{\mathfrak{A}_n^{\mathrm{ab}}}\}$$

である．

例 3.54（正二面体群のアーベル化） 自然数 $n \geq 3$ に対して，n 次の正二面体群 D_n を考える．

$$D_n = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \ldots, \sigma^{n-1}\tau\}$$

であり，$\sigma^n = \tau^2 = 1$，$\tau\sigma = \sigma^{-1}\tau$ であった．このとき，$[D_n, D_n] = \langle\sigma^2\rangle$ である．実際，

$$[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} = \sigma\tau\sigma^{-1}\tau = \sigma\tau\tau\sigma = \sigma^2$$

となるので，$\sigma^2 \in [D_n, D_n]$ となる．したがって，$[D_n, D_n] \supset \langle\sigma^2\rangle$．一方，$D_n$ の任意の交換子を計算すると，

$$\begin{aligned}
[\sigma^i, \sigma^j] &= 1 \\
[\sigma^i, \sigma^j\tau] &= \sigma^i\sigma^j\tau\sigma^{-i}\tau\sigma^{-j} = \sigma^i\sigma^j\tau\tau\sigma^i\sigma^{-j} = \sigma^{2i} \\
[\sigma^i\tau, \sigma^j\tau] &= \sigma^i\tau\sigma^j\tau\tau\sigma^{-i}\tau\sigma^{-j} = \sigma^{2(i-j)}
\end{aligned}$$

となるので，$[D_n, D_n] \subset \langle\sigma^2\rangle$ となることも分かる．よって，n が奇数のとき，$\sigma = \sigma^{n+1} \in \langle\sigma^2\rangle$ であることに注意すれば，

$$[D_n, D_n] = \begin{cases} \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}, & n \text{ が奇数} \\ \{1, \sigma^2, \sigma^4, \ldots, \sigma^{n-2}\}, & n \text{ が偶数} \end{cases}$$

を得る．これより，

$$D_n^{\mathrm{ab}} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & n \text{ が奇数} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & n \text{ が偶数} \end{cases}$$

となる．実際，n が奇数のときは，$|D_n^{\mathrm{ab}}| = 2$ であるから明らか．n が偶数のときは $|D_n^{\mathrm{ab}}| = 4$ である．よって，$D_n^{\mathrm{ab}} \cong \mathbb{Z}/4\mathbb{Z}$ または $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ となる．一方，

$$D_n^{\mathrm{ab}} = \{[D_n, D_n],\ \sigma[D_n, D_n],\ \tau[D_n, D_n],\ \sigma\tau[D_n, D_n]\}$$

であり，すべての元の位数は 2 であるから，$D_n^{\mathrm{ab}} \not\cong \mathbb{Z}/4\mathbb{Z}$．よって，$D_n^{\mathrm{ab}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ となる．

3.6 問題

問題 3.1 $\mathbb{R}$ を実数全体のなす加法群とする．正の実数全体 $\mathbb{R}^+$ を

実数の通常の掛け算により乗法群とみなす．このとき，$\mathbb{R}$ と $\mathbb{R}^+$ は同型であることを示せ．

解答．対数関数 $\log : \mathbb{R}^+ \to \mathbb{R}$，および指数関数 $\exp : \mathbb{R} \to \mathbb{R}^+$ を考える．このとき，

$$\log(xy) = \log(x) + \log(y), \quad x, y \in \mathbb{R}^+$$
$$\exp(x+y) = \exp(x)\exp(y), \quad x, y \in \mathbb{R}$$

が成り立つのでこれらは準同型写像である．さらに，一方が他方の逆写像であるから同型写像である．よって求める結果を得る．□

問題 3.2 G を有限群とする．このとき，ある $n \geq 1$ が存在して，G は n 次対称群 $\mathfrak{S}_n$ の部分群に同型となることを示せ．

解答． $n = |G|$ とする．G の各元 $g \in G$ に対して，写像 $f_g : G \to G$ を，$x \mapsto gx$ によって定める．すると，f_g は全単射である．実際，任意の $y \in G$ に対して，$f_g(g^{-1}x) = g(g^{-1}y) = y$ となるので f は全射．さらに，$x, x' \in G$ に対して，$gx = gx'$ とすれば $x = x'$ となるので f は単射である．したがって，G の各元に $1, 2, \ldots, n$ と番号を振ることによって，各 f_g は $\{1, 2, \ldots, n\}$ 上の置換とみなすことができる．

このとき，写像 $f : G \to \mathfrak{S}_n$ を $g \mapsto f_g$ によって定める．すると，f は単射準同型写像である．実際，$g, g' \in G$ に対して，$f_g = f_{g'}$ とすると，$f_g(1_G) = f_{g'}(1_G)$ より $g = g'$ となるので f は単射．また，任意の $g, g' \in G$ に対して，

$$\begin{aligned} f(gg')(x) &= (gg')x = g(g'x) = g(f_{g'}(x)) \\ &= f_g(f_{g'}(x)) = (f_g \circ f_{g'})(x), \quad x \in G \end{aligned}$$

となるので $f(gg') = f_g \circ f_{g'}$ となり，f は準同型写像である．

以上より，準同型定理を考えると，G は $\mathfrak{S}_n$ の部分群である $\mathrm{Im}(f)$ と同型になることが分かる．□

問題 3.3 R を可換環とし，$R^\times$ を R の単元全体の集合とする．$R^\times$ を R の乗法により乗法群とみなす．$n \geq 2$ を自然数とする．このと

き，以下を示せ．

(1) $\mathrm{SL}(n,R)$ は $\mathrm{GL}(n,R)$ の正規部分群である．

(2) $\mathrm{GL}(n,R)/\mathrm{SL}(n,R) \cong R^\times$.

解答． (1) 行列式写像 $\det : \mathrm{GL}(n,R) \to R^\times$ は準同型写像であり，$\mathrm{SL}(n,R) = \mathrm{Ker}(\det)$ であるから，$\mathrm{SL}(n,R)$ は $\mathrm{GL}(n,R)$ の正規部分群である．

(2) 任意の $u \in R^\times$ に対して，

$$A = \begin{pmatrix} u & O \\ O & E_{n-1} \end{pmatrix} \in \mathrm{GL}(n,R)$$

に対して，$\det(A) = u$ となるので $\det$ は全射である．ゆえに，準同型定理から求める結果を得る．□

問題 3.4 G を群とする．$n \geq 2$ を自然数とし，$\mathbb{Z}/n\mathbb{Z}$ を位数 n の加法群とする．また，$G(n)$ を

$$G(n) := \langle x^n \mid x \in G \rangle$$

で定義される正規部分群とする．このとき，任意の準同型写像 $f : G \to \mathbb{Z}/n\mathbb{Z}$ は，準同型写像 $\overline{f} : G/G(n) \to \mathbb{Z}/n\mathbb{Z}$ を誘導することを示せ．

解答． $G(n) \subset \mathrm{Ker}(f)$ を示せばよい．そこで，$g \in G(n)$ を任意にとる．すると，

$$g = x_1^n x_2^n \cdots x_m^n, \quad x_i \in G$$

とかけるので，

$$f(g) = f(x_1^n x_2^n \cdots x_m^n) = n(f(x_1) + f(x_2) + \cdots + f(x_m)) = 0 \in \mathbb{Z}/n\mathbb{Z}$$

であるから，$G(n) \subset \mathrm{Ker}(f)$ となる．□

問題 3.5 G, H を群として直積群 $G \times H$ を考える．$G \times H$ の部分集合

$$G' := \{(g, 1_H) \in G \times H \mid g \in G\} \subset G \times H$$

を考える．このとき，G' は $G \times H$ の部分群で G と同型であること示せ（H に関しても同様のことが成り立つ）．

解答. G' が $G \times H$ の部分群であることは，$(1_G, 1_H) \in G'$ であり，任意の $(g, 1_H), (g', 1_H) \in G'$ に対して，

$$(g, 1_H)(g', 1_H) = (gg', 1_H), \quad (g, 1_H)^{-1} = (g^{-1}, 1_H) \in G'$$

となることから従う．一方，写像 $f : G \to G'$ を $g \mapsto (g, 1_H)$ で定めれば f は同型写像となる．よって，$G \cong G'$ である．□

問題 3.6 位数 36 のアーベル群の同型類をすべて求めよ．

解答. 36 の素因数は 2 と 3 である．よって，36 を 2 の冪乗と 3 の冪乗の積として表す表し方を考えればよい．すると，

$$12 = 2^2 \times 3^2,\ 2^2 \times 3 \times 3,\ 2 \times 2 \times 3^2,\ 2 \times 2 \times 3 \times 3$$

の 4 通りの場合があるので，位数 36 のアーベル群の相異なる同型類は

$$\mathbb{Z}/36\mathbb{Z},\ \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

の 4 つのみである．□

問題 3.7 $G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ とおく．

(1) G の元で位数が 6 となるものをすべて求めよ．
(2) $\mathbb{Z}/6\mathbb{Z}$ から G への単射準同型写像はいくつかるか．
(3) G の部分群で $\mathbb{Z}/6\mathbb{Z}$ と同型なものはいくつあるか．

解答. (1) $(i, j) \in G$ を位数 6 の元とする．$i = 0$ のとき j は $\mathbb{Z}/6\mathbb{Z}$ の位数 6 でなければならない．よって $j = 1$ または 5．$i = 1$ または 5 のとき，任意の j に対して (i, j) は位数 6 の元である．$i = 2$ とすると i は $\mathbb{Z}/6\mathbb{Z}$ の位数 3 の元であるから，j が $\mathbb{Z}/6\mathbb{Z}$ の 0 または位数 3 の元以外のとき (i, j) は位数 6 の元である．よって，この場合の j の取りうる値は $j = 1, 3, 5$．同様に，$i = 4$ のときも $j = 1, 3, 5$．最後に，$i = 3$ とすると i は $\mathbb{Z}/6\mathbb{Z}$ の位数 2 の元であるから，j が

$\mathbb{Z}/6\mathbb{Z}$ の 0 または位数 2 の元以外のとき (i,j) は位数 6 の元である．よって，この場合の j の取りうる値は $j=1,2,4,5$．以上より，

$$
\begin{aligned}
(i,j) =&(0,1),(0,5),(1,0),(1,1),(1,2),(1,3),(1,4),(1,5)\\
&(2,1),(2,3),(2,5),(3,1),(3,2),(3,4),(3,5),\\
&(4,1),(4,3),(4,5),(5,0),(5,1),(5,2),(5,3),(5,4),(5,5)
\end{aligned}
$$

となる．

(2) $\mathbb{Z}/6\mathbb{Z}$ から G への単射準同型は，$\mathbb{Z}/6\mathbb{Z}$ の生成元 $[1]_6$ に，G の位数 6 の元を一つ対応させるごとに決まる．つまり，$[1]_6$ に (1) で求めた (i,j) を対応させる場合の数だけあり，それは全部で 24 個ある．

(3) H を G の部分群で $\mathbb{Z}/6\mathbb{Z}$ と同型なものとすると，ある同型写像 $\mathbb{Z}/6\mathbb{Z} \to H$ が存在する．すなわち，単射準同型 $\mathbb{Z}/6\mathbb{Z} \to G$ が存在する．したがって，単射準同型 $\mathbb{Z}/6\mathbb{Z} \to G$ であって，像が異なるものがいくつあるかを調べればよい．すると，

$$
\begin{aligned}
H_1 &:= \{(0,j) \mid j \in \mathbb{Z}/6\mathbb{Z}\}\\
H_2 &:= \{(i,0) \mid i \in \mathbb{Z}/6\mathbb{Z}\}\\
H_3 &:= \{(i,i) \mid i \in \mathbb{Z}/6\mathbb{Z}\}\\
H_4 &:= \{(0,0),(1,2),(2,4),(3,0),(4,2),(5,4)\}\\
H_5 &:= \{(0,0),(1,3),(2,0),(3,3),(4,0),(5,3)\}\\
H_6 &:= \{(0,0),(1,4),(2,2),(3,0),(4,4),(5,2)\}\\
H_7 &:= \{(0,0),(1,5),(2,4),(3,3),(4,2),(5,1)\}\\
H_8 &:= \{(0,0),(2,1),(4,2),(0,3),(2,4),(4,5)\}\\
H_9 &:= \{(0,0),(2,3),(4,0),(0,3),(2,0),(4,3)\}\\
H_{10} &:= \{(0,0),(2,5),(4,4),(0,3),(2,2),(4,1)\}\\
H_{11} &:= \{(0,0),(3,1),(0,2),(3,3),(0,4),(3,5)\}\\
H_{12} &:= \{(0,0),(3,2),(0,4),(3,0),(0,2),(3,4)\}
\end{aligned}
$$

の 12 個あることが分かる．□

問題 3.8 以下の位数が等しい群が同型でないことを示せ．

(1) $\mathbb{Z}/3\mathbb{Z} \times \mathfrak{S}_3$ と D_9．
(2) $\mathfrak{S}_3 \times \mathfrak{S}_3$ と D_{18}．

解答． (1) アーベル化を比べればよい．

$$(\mathbb{Z}/3\mathbb{Z} \times \mathfrak{S}_3)^{\mathrm{ab}} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

であり,

$$D_9^{\mathrm{ab}} \cong \mathbb{Z}/2\mathbb{Z}$$

であるから直ちに求める結果を得る.

(2) アーベル化では区別できないので別のことを考える. D_{18} には位数が 18 の元が存在する. もしこの二つの群が同型であれば, $\mathfrak{S}_3 \times \mathfrak{S}_3$ にも位数 18 の元が存在しなければならない. ところが, $\mathfrak{S}_3 \times \mathfrak{S}_3$ の任意の元は 6 乗すると単位元になるので位数は 6 以下である. よって, 二つの群は同型でない. □

4 共役類

この章では，共役という同値関係の下で群の元を分類することを考える．この同値関係による同値類を共役類といい，与えられた群がどのような共役類に分割されるかを決定することは，その群の構造を調べる上で非常に重要な問題である．

4.1 共役類分割

定義 4.1 (共役) G を群とする．$x, y \in G$ に対して，ある $g \in G$ が存在して

$$x = gyg^{-1}$$

となるとき，x と y は**共役** (conjugate) であるといい，$x \sim_c y$ と表す[38]．

すると，$\sim_c$ は G 上に一つの同値関係を定める．実際，任意の $x \in G$ に対して，$x = 1 \cdot x \cdot 1^{-1}$ と書けるので，x と x は共役．また，x と y が共役であるとすると，ある g が存在して，$x = gyg^{-1}$ と書けるが，この両辺に左から g^{-1}，右から g を掛けることで，$y = g^{-1}x(g^{-1})^{-1}$ と書けるので，y と x は共役．さらに，x と y および，y と z がそれぞれ共役であるとすると，ある g, h が存在して，$x = gyg^{-1}$，$y = hzh^{-1}$ となる．よって，$x = (gh)x(gh)^{-1}$ となるので，x と z は共役．以上より，G 上の共役という関係は同値関係である．以下，$x \in G$ の属する同値類を $C(x)$ と書き，x の属する**共役類** (conjugacy class) という．

38) $\sim_c$ なる記号は本書で便宜的に用いるもので一般的ではない．

補題 4.2 G を群とし，$x \in G$ とする．このとき，

$$C(x) = \{x\} \iff x \in Z(G)$$

が成り立つ．したがって，G の中心は，x の属する共役類が x のみからなるような，元 x たちからなる G の部分群である．

証明. ($\Longrightarrow$) 任意の $g \in G$ に対して，$gxg^{-1} \in C(x)$ であるから，$gxg^{-1} = x$ となる．よって，$gx = xg$ となり，$x \in Z(G)$ である．
($\Longleftarrow$) 逆に，$x \in Z(g)$ とすると，任意の g に対して $gx = xg$ が成り立つので，$gxg^{-1} = x$ を得る．これは，G において，x と共役な元は x のみであることを示している．ゆえに，$C(x) = \{x\}$ となる．
□

G がアーベル群のときは明らかに $Z(G) = G$ である．ゆえに，G がアーベル群のときは任意の $x \in G$ に対して $C(x) = \{x\}$ となり，共役類を考える意味がない．

定義 4.3（類等式） 群 G において，共役という同値関係 $\sim_c$ による同値類分割

$$G = Z(G) \cup \bigcup_{\lambda \in \Lambda} C(x_\lambda)$$

を G の**共役類分割** (partition of G into conjugacy classes) という．

特に G が位数 n の有限群の場合，G は有限個の共役類に分割できる．このとき $|Z(G)| = z$, $|C(x_i)| = l_i$ とおくと，

$$n = z + l_1 + \cdots + l_m$$

なる等式が得られる．これを G の**類等式** (class formula) という．

定理 4.4 G を群とし，$x \in G$ とする．

(1) 剰余類の集合 $G/C_G(x)$（一般に剰余群とは限らない.）を考える．このとき，$|G/C_G(x)| = |C(x)|$ が成り立つ．
(2) 特に G が有限群の場合，$|C(x)|$ は G の位数 $|G|$ の約数である．

証明. (1) 写像 $f : G/C_G(x) \to C(x)$ を

$$gC_G(x) \mapsto gxg^{-1}$$

によって定義する．まず，f が well-defined であることを示す．そこで，$g, h \in G$ を $gC_G(x) = hC_G(x)$ なる元とすると，ある $r \in C_G(x)$ が存在して，$h = gr$ と書ける．このとき，r と x は可換であるから

$$f(hC_G(x)) = hxh^{-1} = grxr^{-1}g^{-1} = gxg^{-1} = f(gC_G(x))$$

となる．よって，f は well-defined である．

次に，f が全単射であることを示そう．任意の $y \in C(x)$ に対して，ある $g \in G$ が存在して，$y = gxg^{-1}$ と書ける．よって，このとき，$f(gC_G(x)) = gxg^{-1} = y$ となるので f は全射である．一方，$gC_G(x), hC_G(x) \in G/C_G(x)$ に対して，$f(gC_G(x)) = f(hC_G(x))$ と仮定すると，$gxg^{-1} = hxh^{-1}$ となる．よって，$(h^{-1}g)x = x(h^{-1}g)$ となり，$h^{-1}g \in C_G(x)$ を得る．すなわち，$gC_G(x) = hC_G(x)$ となり，f は単射であることが分かる．

以上より，f は全単射となり求める等式を得る．

(2) G を有限群とする．(1) より，$|C(x)| = |G/C_G(x)|$ であり，$|G/C_G(x)|$ は G の位数の約数であるから直ちに求める結果を得る．
□

定理 4.5 G を有限群，H を G の部分群とし，T を G の部分集合とする．$C_H(T) := \{hTh^{-1} \mid h \in H\}$ とおく．このとき，

$$|C_H(T)| = |H/(H \cap N_G(T))|$$

が成り立つ．ここで，$H/(H \cap N_G(T))$ は剰余類の集合である．

特に，$H = G$ のとき，$C(T) := C_G(T)$ とおくと，

$$|C(T)| = |G/N_G(T)|$$

が成り立つ．

証明. 写像 $f : H/(H \cap N_G(T)) \to C_H(T)$ を

$$h(H \cap N_G(T)) \mapsto hTh^{-1}$$

によって定める．すると，これは well-defined である．実際，$h(H \cap N_G(T)) = h'(H \cap N_G(T))$ とすると，ある $k \in (H \cap N_G(T))$ が存

在して $h' = hk$ となる．このとき，

$$f(h'(H \cap N_G(T))) = h'T(h')^{-1} = hkTk^{-1}h^{-1} = hTh^{-1}$$
$$= f(h(H \cap N_G(T)))$$

となる．

f が全単射になることを示そう．任意の $T' \in C_H(T)$ に対して，ある $h \in H$ が存在して $T' = hTh^{-1}$ となる．よって，$T' = f(h(H \cap N_G(T)))$ となり，f は全射である．また，$h(H \cap N_G(T)), h'(H \cap N_G(T))$ に対して，$f(h(H \cap N_G(T))) = f(h'(H \cap N_G(T)))$ とすると，$hTh^{-1} = h'T(h')^{-1}$ であるから，$h^{-1}h'T = Th^{-1}h'$ となる．つまり，$h^{-1}h' \in H \cap N_G(T)$ であり，$g(H \cap N_G(T)) = g'(H \cap N_G(T))$ を得る．つまり，f は単射である．以上より，求める等式が導かれる．
□

定義 4.6（共役部分群） G を群とし，H を部分群とする．このとき，任意の $g \in G$ に対して，H の共役集合 gHg^{-1} は G の部分群である．実際，$1_G = g1_Gg^{-1} \in gHg^{-1}$ となるので，$gHg^{-1} \neq \emptyset$．さらに，$x, y \in gHg^{-1}$ とすると，ある $s, t \in H$ が存在して，$x = gsg^{-1}$，$y = gtg^{-1}$ と書ける．このとき，$xy = (gsg^{-1})(gtg^{-1}) = g(st)g^{-1}$ となるが，H が部分群であるので $st \in H$．したがって，$xy \in gHg^{-1}$ である．一方，任意の $x \in gHg^{-1}$ に対して，$x = gsg^{-1}$ $(s \in H)$ とおくとき，$x^{-1} = gs^{-1}g^{-1}$ であり，$s^{-1} \in H$ であるから $x^{-1} \in gHg^{-1}$ となる．ゆえに，gHg^{-1} は G の部分群である．この gHg^{-1} を G における H の**共役部分群** (conjugate subgroup) という．

明らかに，H は H の共役部分群である．実際，$g = 1_G$ とすれば，$H = 1_GH1_G^{-1}$ である．

命題 4.7 G を群とし，H を部分群とする．このとき以下が成り立つ．

$$H \lhd G \iff H \text{ の共役部分群は } H \text{ のみ}$$

証明. $(\Longrightarrow)$ H が G の正規部分群であるとき，任意の $g \in G$ に対して，$gHg^{-1} = H$ である．すなわち，H の共役部分群は H のみである．

$(\Longleftarrow)$ 任意の $g \in G$ に対して，gHg^{-1} は H の共役部分群であるの

で，仮定より $gHg^{-1} = H$ となる．これは H が G の正規部分群であることを示している．□

4.2 有限群の類等式の例

本節では，これまでに述べた群に関する類等式の簡単な例をいくつか解説する．

4.2.1 正二面体群の類等式

まず手頃な例として正二面体群を考えよう．$n \geq 3$ に対して，D_n の共役類は，

(1) n が偶数のとき，

$$\{1\},\ \{\sigma, \sigma^{-1}\},\ \{\sigma^2, \sigma^{-2}\}, \ldots, \{\sigma^{\frac{n-2}{2}}, \sigma^{\frac{2-n}{2}}\},\ \{\sigma^{\frac{n}{2}}\},$$
$$\{\tau, \sigma^2\tau, \ldots, \sigma^{n-2}\tau\},\ \{\sigma\tau, \sigma^3\tau, \ldots, \sigma^{n-1}\tau\}$$

(2) n が奇数のとき，

$$\{1\},\ \{\sigma, \sigma^{-1}\},\ \{\sigma^2, \sigma^{-2}\}, \ldots, \{\sigma^{\frac{n-1}{2}}, \sigma^{\frac{1-n}{2}}\},$$
$$\{\tau, \sigma\tau, \ldots, \sigma^{n-1}\tau\}$$

である．実際, n が偶数のときを考えてみよう．任意の $1 \leq i \leq n-1$ に対して，σ^i の共役元を調べる．すると，任意の $x \in D_n$ に対して，

$$x\sigma^i x^{-1} = \begin{cases} \sigma^j \sigma^i \sigma^{-j} = \sigma^i, & x = \sigma^j \text{ のとき} \\ \sigma^j \tau \sigma^i \tau \sigma^{-j} = \sigma^{-i}, & x = \sigma^j \tau \text{ のとき} \end{cases}$$

となるので, σ^i と共役な元は $\sigma^{\pm i}$ である．次に, 任意の $1 \leq i \leq n-1$ に対して，$\sigma^i \tau$ の共役元を調べる．すると，任意の $x \in D_n$ に対して，

$$x\sigma^i \tau x^{-1} = \begin{cases} \sigma^j \sigma^i \tau \sigma^{-j} = \sigma^{i+2j}\tau, & x = \sigma^j \text{ のとき} \\ \sigma^j \tau \sigma^i \tau \tau \sigma^{-j} = \sigma^{i+2(j-i)}\tau, & x = \sigma^j \tau \text{ のとき} \end{cases}$$

となるので，$\sigma^i \tau$ と共役な元は $\sigma^k \tau$ $(k \equiv i \pmod 2)$ なる形の元である．よって，(1) が得られる．(2) についても同様である．

以上より，D_n の類等式は，

(1) n が偶数のとき，

$$2n = 2 + 2 + 2 + \cdots + 2 + \frac{n}{2} + \frac{n}{2}$$

(2) n が奇数のとき，

$$2n = 1 + 2 + 2 + \cdots + 2 + n$$

となる．また，系として，以下を得る．

系 4.8 $n \geq 3$ に対して，

$$Z(D_n) = \begin{cases} \{1,\ \sigma^{\frac{n}{2}}\}, & n \text{ が偶数のとき} \\ \{1\}, & n \text{ が奇数のとき} \end{cases}$$

となる．

証明. 一般に，群の中心は単独で共役類を形成するような元の集合であるから，上の結果より直ちに導かれる．□

4.2.2 対称群の類等式

次に，対称群の共役類と類等式について考える．対称群の共役類は巡回置換の型と一対一に対応することが知られており，いろいろな応用がある．まず，巡回置換の性質について述べる．

定理 4.9 対称群 $\mathfrak{S}_n$ において以下が成り立つ．

(1) 長さ m の巡回置換 $(a_1\,a_2\,\cdots a_m)$ の位数は m.

(2) 長さ m の巡回置換 $(a_1\,a_2\,\cdots a_m)$ に対して，

$$(a_1\,a_2\,\cdots a_m) = (a_1\,a_m)(a_1\,a_{m-1})\cdots(a_1\,a_2).$$

(3) 互いに共通の数字を含まない二つの巡回置換は $\mathfrak{S}_n$ において可換.

(4) 任意の $\sigma = (a_1\,a_2\,\cdots a_m)$, $\tau \in \mathfrak{S}_n$ に対して，

$$\tau\sigma\tau^{-1} = (\tau(a_1)\,\tau(a_2)\,\cdots\tau(a_m)).$$

証明 (1) $\sigma = (a_1\, a_2\, \cdots a_m)$ とおく．明らかに，$\sigma^m = 1$ である．一方，任意の $1 \leq k \leq m-1$ に対して，$\sigma^k(a_1) = a_k \neq a_1$ であるから，$\sigma^k \neq 1_{\mathfrak{S}_n}$ である．

(2) 右辺の積を σ とおく．このとき，任意の $1 \leq k \leq m-1$ に対して，

$$\begin{aligned}\sigma(a_k) &= (a_1\, a_m)(a_1\, a_{m-1}) \cdots (a_1\, a_{k+1})(a_1\, a_k)(a_k) \\ &= (a_1\, a_m)(a_1\, a_{m-1}) \cdots (a_1\, a_{k+1})(a_1) \\ &= (a_1\, a_m)(a_1\, a_{m-1}) \cdots (a_1\, a_{k+2})(a_{k+1}) \\ &= a_{k+1}\end{aligned}$$

であり，$\sigma(a_m) = a_1$ であるから，$\sigma = (a_1\, a_2\, \cdots a_m)$ となる．

(3) 巡回置換の定義から明らか．

(4) 任意の $1 \leq k \leq m-1$ に対して，

$$\tau\sigma\tau^{-1}(\tau(a_k)) = \tau\sigma(a_k) = \tau(a_{k+1})$$

であり，

$$\tau\sigma\tau^{-1}(\tau(a_m)) = \tau\sigma(a_m) = \tau(a_1)$$

であるから求める結果を得る．□

命題 4.10 任意の元 $\sigma \in \mathfrak{S}_n$ は，互いに共通の数字を含まない巡回置換の積として表せる．

証明 $n \geq 2$ についての帰納法による．$n = 2$ のとき，$\mathfrak{S}_2 = \{1_{\mathfrak{S}_2}, (1\,2)\}$ であるから明らか．そこで，$n \geq 3$ とし，$\sigma \in \mathfrak{S}_n$ を任意にとる．もし，σ が n 次巡回置換であれば示すべきことはないので，σ が n 次の巡回置換でないとする．

任意に $1 \leq a_1 \leq n$ をとる．もし $\sigma(a_1) \neq a_1$ であれば，$a_2 := \sigma(a_1)$ とおく．次に，もし $\sigma(a_2) \neq a_1$ であれば $a_3 = \sigma(a_2)$ とおく．このとき，a_1, a_2, a_3 はすべて相異なる．実際，$a_3 = a_2$ と仮定すると，$\sigma(a_2) = \sigma(a_1)$ より $a_2 = a_1$ となり矛盾．以下，同様の操作を繰り返すことにより，いつかは $\sigma(a_m) = a_1$ なる a_m に到達し，$a_1, a_2, \ldots, a_m$ はすべて相異なるようにできることが m に関する帰納法で証明できる．実際，$a_m = a_1$ となったとすると $\sigma(a_1) \neq a_1$ に矛盾であり，ある $2 \leq i \leq m-1$ に対して $a_m = a_i$ となったとす

ると，$\sigma(a_{m-1}) = \sigma(a_{i-1})$ より $a_{m-1} = a_{i-1}$ となり帰納法の仮定に矛盾である．よって，$a_1, a_2, \ldots, a_m$ はすべて相異なり，このような m は n を超えないのでいつかは $\sigma(a_m) = a_1$ となる．

さて，σ は n 次の巡回置換ではないので $m < n$ である．一方，σ は $\{1, 2, \ldots, n\} \setminus \{a_1, a_2, \ldots, a_m\}$ 上に置換を誘導するのでこれを σ' とおけば，

$$\sigma = (a_1\, a_2\, \cdots a_m)\sigma'$$

であり，帰納法の仮定により σ' は巡回置換の積に表すことができる．よって帰納法が進む．□

定義 4.11（**分解型**）各元 $\sigma \in \mathfrak{S}_n$ を互いに共通の数字を含まない巡回置換の積として $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$ のように表す．このとき，定理 4.9 の (3) により，各巡回置換 σ_i の長さ m_i は

$$m_1 \geq m_2 \geq \cdots \geq m_r$$

であると仮定してよい．このとき，$(m_1, m_2, \ldots, m_r)$ を σ の**分解型** (cycle type) という．

定理 4.12 $\sigma, \sigma' \in \mathfrak{S}_n$ が共役であるためには，σ と σ' の分解型が一致することが必要十分である．

証明（必要性）$\tau \in \mathfrak{S}_n$ に対して，$\sigma' = \tau\sigma\tau^{-1}$ となったとする．σ の互いに共通の数字を含まない巡回置換の積としての表示を

$$\sigma = (a_1\, a_2\, \cdots a_m)(b_1\, b_2\, \cdots b_l) \cdots (c_1\, c_2\, \cdots c_k)$$

とすれば，定理 4.9 の (4) より，

$$\begin{aligned}
\tau\sigma\tau^{-1} &= \tau(a_1\, a_2\, \cdots a_m)\tau^{-1} \cdot \tau(b_1\, b_2\, \cdots b_l)\tau^{-1} \cdots \tau(c_1\, c_2\, \cdots c_k)\tau^{-1} \\
&= (\tau(a_1)\, \tau(a_2)\, \cdots \tau(a_m)) \cdot (\tau(b_1)\, \tau(b_2)\, \cdots \tau(b_l)) \\
&\qquad \cdots (\tau(c_1)\, \tau(c_2)\, \cdots \tau(c_k))
\end{aligned}$$

を得る．したがって，σ と σ' の分解型は一致する．

（十分性）σ と σ' の分解型が一致するとし，それぞれの互いに共通の数字を含まない巡回置換の積としての表示を

$$\sigma = (a_1\, a_2\, \cdots a_m)(b_1\, b_2\, \cdots b_l)\cdots(c_1\, c_2\, \cdots c_k)$$
$$\sigma' = (a'_1\, a'_2\, \cdots a'_m)(b'_1\, b'_2\, \cdots b'_l)\cdots(c'_1\, c'_2\, \cdots c'_k)$$

とする．$m + l + \cdots + k = n$ である．そこで，置換 $\tau \in \mathfrak{S}_n$ を $\tau(x) := x'$ によって定めれば，$\sigma' = \tau\sigma\tau^{-1}$ となるので，σ と σ' は共役である．□

定義 4.13（分割数） 任意の自然数 $n \geq 1$ に対して，n を自然数の和として

$$n = m_1 + m_2 + \cdots + m_r, \quad (m_1 \geq m_2 \geq \cdots \geq m_r)$$

なる形に表すときの総数を n の**分割数** (partition number) といい，$P(n)$ と書く．

例 4.14 例えば，$n = 4$ のとき，

$$4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$$

であるから $P(4) = 5$ である．同様にして，$P(1) = 1$, $P(2) = 2$, $P(3) = 3$ である．

定理 4.12 の系として以下が従う．

系 4.15 対称群 $\mathfrak{S}_n$ の共役類の個数は分割数 $P(n)$ に等しい．

ここで，4 次対称群の共役類に関する例を考えてみよう．

例題 4.16 $\mathfrak{S}_4$ の共役類と類等式を求めよ．

解答. 巡回置換による分解型とそれに対する共役類は全部で

分解型	共役類	置換	個数
(1,1,1,1)	$C_1 := \{1\}$	偶	1
(2,1,1)	$C_2 := \{(1\,2),(1\,3),(1\,4),(2\,3),(2\,4),(3\,4)\}$	奇	6
(2,2)	$C_3 := \{(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\}$	偶	3
(3,1)	$C_4 := \{(1\,2\,3),(1\,2\,4),(1\,3\,2),(1\,3\,4),$ $(1\,4\,2),(1\,4\,3),(2\,3\,4),(2\,4\,3)\}$	偶	8
(4)	$C_5 := \{(1\,2\,3\,4),(1\,2\,4\,3),(1\,3\,2\,4),$ $(1\,3\,4\,2),(1\,4\,2\,3),(1\,4\,3\,2)\}$	奇	6

となる．よって，類等式は

$$24 = 1 + 6 + 3 + 8 + 6$$

となる．□

4.2.3 交代群の共役類

対称群の共役類分割を利用して交代群の共役類分割を求めよう．一般に，$\mathfrak{A}_n$ 内で共役な二つの元は $\mathfrak{S}_n$ 内でも共役であるから，$\mathfrak{A}_n$ の共役類は，$\mathfrak{S}_n$ のある共役類で偶置換から成るものに含まれることが分かる．したがって，$\mathfrak{A}_n$ の共役類を求めるためには，$\mathfrak{S}_n$ の偶置換からなる共役類たちが，$\mathfrak{A}_n$ 内で見たときにどのように分裂するかを調べればよい．

そこで，C を $\mathfrak{S}_n$ の偶置換からなる共役類とし，$\sigma \in C$ とする．このとき，

$$N_{\mathfrak{A}_n}(\{\sigma\}) = N_{\mathfrak{S}_n}(\{\sigma\}) \cap \mathfrak{A}_n$$

が成り立つ．以下二つの場合に分ける．

(1) $N_{\mathfrak{S}_n}(\{\sigma\})$ が奇置換を含む場合．

このときは，$\mathfrak{S}_n = \mathfrak{A}_n N_{\mathfrak{S}_n}(\{\sigma\})$ である．よって，第 2 同型定理を用いて

$$\begin{aligned}[\mathfrak{S}_n : N_{\mathfrak{S}_n}(\{\sigma\})] &= [\mathfrak{A}_n N_{\mathfrak{S}_n}(\{\sigma\}) : N_{\mathfrak{S}_n}(\{\sigma\})] \\ &= [\mathfrak{A}_n : N_{\mathfrak{S}_n}(\{\sigma\}) \cap \mathfrak{A}_n] \\ &= [\mathfrak{A}_n : N_{\mathfrak{A}_n}(\{\sigma\})]\end{aligned}$$

となる．ここで，定理 4.5 より，$[\mathfrak{S}_n : N_{\mathfrak{S}_n}(\{\sigma\})]$ は $\mathfrak{S}_n$ において σ と共役な元の個数（つまり $|C|$.），および $[\mathfrak{A}_n : N_{\mathfrak{A}_n}(\{\sigma\})]$ は $\mathfrak{A}_n$ において σ と共役な元の個数であり，上の関係から両者は一致する．したがって，C 自身が $\mathfrak{A}_n$ の一つの共役類になっている．

(2) $N_{\mathfrak{S}_n}(\{\sigma\})$ が奇置換を含まない場合．

このときは，$N_{\mathfrak{S}_n}(\{\sigma\}) \subset \mathfrak{A}_n$ であり，$N_{\mathfrak{S}_n}(\{\sigma\}) = N_{\mathfrak{A}_n}(\{\sigma\})$ である．よって，

$$\begin{aligned}[\mathfrak{S}_n : N_{\mathfrak{A}_n}(\{\sigma\})] &= [\mathfrak{S}_n : \mathfrak{A}_n][\mathfrak{A}_n : N_{\mathfrak{A}_n}(\{\sigma\})] \\ &= 2[\mathfrak{A}_n : N_{\mathfrak{A}_n}(\{\sigma\})]\end{aligned}$$

より，$\mathfrak{A}_n$ の中で σ を含む共役類 $C_{\mathfrak{A}_n}(\{\sigma\})$ の元の個数は C の

元の個数の丁度半分である．また，$\tau \in C$ を $\mathfrak{A}_n$ の中で σ と共役でない元とすると，同様の議論により τ を含む $\mathfrak{A}_n$ の共役類 $C_{\mathfrak{A}_n}(\{\tau\})$ の元の個数もは C の元の個数の丁度半分である．さらに，$C_{\mathfrak{A}_n}(\{\sigma\}) \cap C_{\mathfrak{A}_n}(\{\tau\}) = \emptyset$，$C = C_{\mathfrak{A}_n}(\{\sigma\}) \cup C_{\mathfrak{A}_n}(\{\tau\})$ であるので，C は $\mathfrak{A}_n$ において元の個数が等しい二つの共役類に分裂する．

以上の議論を踏まえて，$\mathfrak{A}_4$ の共役類を具体的に考察してみよう．以下に示すように，実際には正規化群に注目しなくても直接的な計算により求めることもできる（しかしながら，検算にもなるので上の事実はよく理解しておくべきである）．

例題 4.17 $\mathfrak{A}_4$ の共役類と類等式を求めよ．

解答． まず $\mathfrak{S}_4$ の共役類で偶置換からなるものを考える．すると，それらは，

$C_1 := \{1\}$

$C_2 := \{(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$

$C_3 := \{(1\,2\,3), (1\,2\,4), (1\,3\,2), (1\,3\,4), (1\,4\,2), (1\,4\,3), (2\,3\,4), (2\,4\,3)\}$

である．すると，C_2 は $\mathfrak{A}_4$ でも共役類である．実際，計算により

$$(1\,2\,3)\,(1\,2)(3\,4)\,(1\,2\,3)^{-1} = (1\,4)(2\,3)$$
$$(1\,3\,2)\,(1\,2)(3\,4)\,(1\,3\,2)^{-1} = (1\,3)(2\,4)$$

であることが確かめられる．

一方，$|C_3| = 8$ であり，$8 \nmid |\mathfrak{A}_4|$ であるから，C_3 はいくつかの $\mathfrak{A}_4$ の共役類に分解する（実は二つである）．すると，

$$(1\,2)(3\,4)\,(1\,2\,3)\,(3\,4)(1\,2) = (1\,4\,2)$$
$$(1\,3)(2\,4)\,(1\,2\,3)\,(2\,4)(1\,3) = (1\,3\,4)$$
$$(1\,4)(2\,3)\,(1\,2\,3)\,(2\,3)(1\,4) = (2\,4\,3)$$

であるから，計算により

$$C_{31} := \{(1\,2\,3), (1\,4\,2), (1\,3\,4), (2\,4\,3)\}$$

が $\mathfrak{A}_4$ の一つの共役類であることが分かる．したがって，残りはもう一つの共役類

$$C_{32} := \{(1\,3\,2), (1\,2\,4), (1\,4\,3), (2\,3\,4)\}$$

となる．よって，C_1, C_2, C_{31}, C_{32} が求める共役類で，類等式は $1 + 3 + 4 + 4$ となる．□

例 4.18 $\mathfrak{A}_4$ には位数 6 の部分群が存在しないことが以下のようにして示される．

$\mathfrak{A}_4$ に位数 6 の部分群 N が存在したとする．すると $[\mathfrak{A}_4 : N] = 2$ であるから，N は $\mathfrak{A}_4$ の正規部分群である．したがって，N は $\mathfrak{A}_4$ の共役類をいくつか合わせたものである．ところが，$\mathfrak{A}_4$ の共役類は全部で四つあり，それらに含まれる元の個数は 1, 3, 4, 4 である．これらをどのように足しても 6 にはならないのでこれは矛盾である．すなわち，$\mathfrak{A}_4$ に位数 6 の部分群は存在しない．

例 4.19 4 次の交代群 $\mathfrak{A}_4$ のアーベル化について考察しよう．簡単な計算により，

$$[(123), (124)] = (12)(34), \quad [(132), (134)] = (13)(24),$$
$$[(143), (142)] = (14)(23)$$

であることが分かる．したがって，単位元のことも考えると，$|[\mathfrak{A}_4, \mathfrak{A}_4]| \geq 4$ であることが分かる．一方，$\mathfrak{A}_4$ の部分群の位数は $1, 2, 3, 4, 6$ のいずれかであるが，例 4.18 により，$1, 2, 3, 4$ となることが分かる．したがって，$|[\mathfrak{A}_4, \mathfrak{A}_4]| = 4$ であり，特に

$$[\mathfrak{A}_4, \mathfrak{A}_4] = \{1_{\mathfrak{A}_4}, (12)(34), (13)(24), (14)(23)\}$$

である．よって，$|\mathfrak{A}_4^{\mathrm{ab}}| = 3$ となり，$\mathfrak{A}_4^{\mathrm{ab}} \cong \mathbb{Z}/3\mathbb{Z}$ であることが分かる．

4.3 問題

問題 4.1 $\mathfrak{S}_3$ の共役類と類等式を求めよ．

解答. 巡回置換による分解型とそれに対する共役類は全部で

分解型	共役類	置換	個数
$(1,1,1)$	$C_1 := \{1\}$	偶	1
$(2,1)$	$C_2 := \{(1\,2), (1\,3), (2\,3)\}$	奇	3
(3)	$C_3 := \{(1\,2\,3), (1\,3\,2)\}$	偶	2

となる．よって，類等式は $6 = 1 + 3 + 2$ となる．□

問題 4.2 $\mathfrak{A}_5$ の共役類と類等式を求めよ．

解答. しらみ潰しに計算すると，求める共役類は

$$C_1 := \{1\},\ C_2 := C_{\mathfrak{S}_5}((1\,2)(3\,4)),\ C_3 := C_{\mathfrak{S}_5}((1\,2\,3))$$
$$C_4 := \{(1\,2\,3\,4\,5), (1\,2\,4\,5\,3), (1\,2\,5\,3\,4), (1\,3\,2\,5\,4), (1\,3\,5\,4\,2), (1\,3\,4\,2\,5), (1\,4\,3\,5\,2), (1\,4\,5\,2\,3), (1\,4\,2\,3\,5), (1\,5\,2\,4\,3), (1\,5\,4\,3\,2), (1\,5\,3\,2\,4)\}$$
$$C_5 := \{(1\,2\,4\,3\,5), (1\,2\,5\,4\,3), (1\,2\,3\,5\,4), (1\,3\,5\,2\,4), (1\,3\,4\,5\,2), (1\,3\,2\,4\,5), (1\,4\,5\,3\,2), (1\,4\,2\,5\,3), (1\,4\,3\,2\,5), (1\,5\,4\,2\,3), (1\,5\,3\,4\,2), (1\,5\,2\,3\,4)\}$$

の 5 個であることが分かる．よって，類等式は $60 = 1 + 15 + 20 + 12 + 12$ となる．□

5 変換群

一般に，群の性質を調べようとする際に，与えられた群だけを調べるのではなく，その群が作用するような集合をあわせて考えること議論が鮮明かつスムーズになることがある．つまり，群が集合に作用する様子を考察することで群のより詳しい性質や情報を得ようというのである．例えば，位相幾何学においては，与えられた群が作用するような“よい”位相空間を見つけてきて，その作用の様子から元の群の生成元やその間の関係式などを考察することがある．この章では，シローの定理に必要となる事項に限定して群の作用について解説をする．

5.1 群の作用

定義 5.1（変換群） G を群，X を集合とする．任意の $g \in G$ と任意の $x \in X$ に対して，ある $g \cdot x \in X$ が一意的に定義されていて，

(1) 任意の $g, h \in G$ と任意の $x \in X$ に対して，$g \cdot (h \cdot x) = (gh) \cdot x$ が成り立つ．

(2) 任意の $x \in X$ に対して，$1_G \cdot x = x$.

を満たすとき，G は X に（左から）**作用する** (act) といい，$G \curvearrowright X$ と表す．このとき，G を X の**変換群** (transformation group) といい，X は **G-同変な集合** (G-equivariant set)，または単に **G 集合** (G-set) とも呼ばれる．

注意 5.2 群 G の集合 X への作用が与えられたとき，写像 ρ : $G \times X \to X$ を $\rho(g,x) := g \cdot x$ で定めれば，

(1) 任意の $g,h \in G$ と任意の $x \in X$ に対して，$\rho(g,\rho(h,x)) = \rho(gh,x)$,
(2) 任意の $x \in X$ に対して，$\rho(1_G,x) = x$.

を満たす．逆に，上の性質を満たす写像 $\rho : G \times X \to X$ が与えられれば，$g \cdot x := \rho(g,x)$ とおくことにより，G の X への作用が一つ定まる．

すなわち，群 G の集合 X への作用を考えることと，上記の性質を満たす写像 $\rho : G \times X \to X$ を考えることは本質的に同値である．以下，単に群 G の集合 X への作用といえば，このような写像を指すものとする．

定義 5.3（自明な作用） G を群，X を集合とする．任意の $g \in G$ と任意の $x \in X$ に対して $g \cdot x := x$ と定めると，明らかにこれは G の X への作用を与える．このような作用を**自明な作用** (trivial action) という．

定義 5.4（G-軌道） G を群，X を G-集合とする．このとき，X 上に関係[39] $\sim_o$ を $x,y \in X$ に対して，

$$x \sim_o y \iff \text{ある } g \in G \text{ が存在して，} x = g \cdot y \text{ となる．}$$

と定める．するとこれは X 上の一つの同値関係を定める．

この同値関係 $\sim_o$ による X の同値類を X の **G-軌道** (G-orbit) という．特に，$x \in X$ の属する G-軌道を G_x と表すことにする．G-軌道全体の集合を $G \backslash X$ と書く．

[39] 記号 $\sim_o$ は本書のみで用いる便宜的な記号である．

定義 5.5（固定点） G を群，X を G-集合とする．任意の $g \in G$ に対して，$g \cdot x = x$ となるような点 $x \in X$ を**固定点** (fixed point) という．

定義 5.6（固定化群） G を群，X を G-集合とする．このとき，各 $x \in X$ に対して，G の部分集合

$$S_G(x) := \{g \in G \mid g \cdot x = x\} \subset G$$

は G の部分群になる．これを，x の**固定化群** (stabilizer) [40] という．

[40] **安定化群**ということもある．

定理 5.7 G を群，X を G-集合とする．このとき，各 $x \in X$ に対して，

$$|G/S_G(x)| = |Gx|$$

が成り立つ．ここで，$G/S_G(x)$ は剰余類の集合（一般に，$S_G(x)$ は G の正規部分群とは限らないので，$G/S_G(x)$ が群構造を持つかどうか分からない）であり，上の等式は濃度の意味で成り立つ．特に，G が有限群のときは，$|Gx|$ は $|G|$ の約数である．

証明. 写像 $f : G/S_G(x) \to Gx$ を

$$gS_G(x) \mapsto g \cdot x$$

で定義する．すると，これは well-defined である．実際，$gS_G(x) = g'S_G(x)$ とすると，ある元 $s \in S_G(x)$ が存在して，$g' = gs$ となる．このとき，

$$f(g'S_G(x)) = g' \cdot x = gs \cdot x = g \cdot (s \cdot x) = g \cdot x = f(gS_G(x))$$

となる．

次に，f が全単射であることを示そう．任意の $y \in Gx$ に対して，y は x の G-軌道の元であるから，ある $G \in G$ が存在して，$y = g{\cdot}x$ となる．ゆえに，$y = f(g)$ となり，f は全射．一方，$f(gS_G(x)) = f(g'S_G(x))$ とすると，$g \cdot x = g' \cdot x$ であるから，両辺に左から g^{-1} を作用させることにより，$x = (g^{-1}g') \cdot x$ であることが分かる．すなわち，$g^{-1}g' \in S_G(x)$ である．よって，$gS_G(x) = g'S_G(x)$ となり，f は単射である．以上より，f は全単射であり求める結果を得る．□

注意 5.8 定理 5.7 は，群の構造をその群が作用する集合を通して調べられることを示している．章の初めに，位相幾何学では与えられた群の構造を調べるために，その群が作用するような "よい" 位相空間を見つけることが重要であると述べたが，特に，各固定化群ができるだけ小さくなるようなものが望ましく，理想的なのは各固定化

群が自明な場合である．この意味において，初等的ではあるが，上の定理は代数学（群論）と幾何学（位相幾何学）を繋ぐ定理といえよう．

定義 5.9（自由な作用） G を群，X を G-集合とする．各 $x \in X$ に対して，x の固定化群が自明のとき，すなわち $S_G(x) = \{1_G\}$ となるとき，G の X への作用は**自由** (free) であるという．

定義 5.10（軌道分解） G を群，X を G-集合とする．X 上の同値関係 $\sim_o$ による X の同値類別

$$X = \coprod_{\lambda \in \Lambda} G_{x_\lambda} \text{（直和）} \tag{5.1}$$

を X の G-**軌道分解** (orbit decomposition) という[41]．

また，$|X| = n < \infty$ のとき，$|G_{x_\lambda}| = l_\lambda$ として，

$$n = \sum_{\lambda \in \Lambda} l_\lambda$$

を X の G-**軌道分解等式** (orbit decomposition formula) という．

41) 記号 $\coprod$ は，互いに共通部分を持たないような集合の和集合を表すときに用いる，直和を表す記号である．

注意 5.11 群 G に対して，G の G への作用を

$$g \cdot x := gxg^{-1}, \quad g, x \in G$$

によって定める．これを，G の**共役作用** (conjugate action) という．このとき，G の共役類分割，類等式はそれぞれ，G の共役作用による軌道分解，軌道分解等式にほかならない．

定義 5.12（推移的） G を群，X を G-集合とする．X の G 軌道が G のみであるとき，G の X への作用は**推移的** (transitive) であるという．すなわち，任意の $x, y \in X$ に対して，ある $g \in G$ が存在して，$x = g \cdot y$ となるとき，G の X への作用は推移的である．

注意 5.13 群 G が X に作用しているとする．すると，G は X の各 G-軌道 G_x に作用するが，この作用は推移的である．実際，任意の $y, z \in G_x$ に対して，$y = g \cdot x$, $z = g' \cdot x$ となる $g, g' \in G$ が存在する．このとき，$g'' := g(g')^{-1} \in G$ とおくと $y = g'' \cdot z$ となる．

次に，群の作用を部分群に制限することを考えよう．

定義 5.14（部分群への制限） G を群，X を G-集合とする．H を G の部分群とする．このとき，任意の $x \in X$ に対して，各 $h \in H$ の x への作用を，$h \in G$ の x への作用を用いて，$h \cdot x \in X$ と定めることにより，H は X へ作用することが分かる．このような作用を，G の作用の H への**制限** (restriction) という．

G の X への作用を与えることは，注意 5.2 における二つの性質を満たすような写像 $\rho : G \times X \to X$ を与えることと同値であった．G の作用を H へ制限することは，写像 $\rho : G \times X \to X$ を $H \times X \subset G \times X$ に制限することにほかならない．

X の G-軌道分解 (5.1) を考える．各 G_{x_λ} の H-軌道分解を $G_{x_\lambda} = \coprod_{\lambda' \in \Lambda'} H_{x_{\lambda,\lambda'}}$ とすれば，X の H-軌道分解

$$X = \coprod_{\lambda \in \Lambda} \coprod_{\lambda' \in \Lambda'} H_{x_{\lambda,\lambda'}}$$

を得る．

定義 5.15（剰余群に誘導される作用） G を群，X を G-集合とする．N を G の正規部分群とし，G の作用の N への制限は自明であるとする．このとき，任意の $x \in X$ に対して，各剰余類 $gN \in G/N$ の x への作用を，

$$(gN) \cdot x := g \cdot x \in X$$

と定めることができる[42]．

[42] ここで，左辺の・は新しく定義しようとしている G/N の X への作用で，右辺の・は G の X への作用である．

実際，この定義が well-defined であることを示そう．そこで，$gN = g'N$ であるとき，ある $n \in N$ が存在して，$g' = gn$ とかける．すると，任意の $x \in X$ に対して，

$$(g'N) \cdot x = g' \cdot x = (gn) \cdot x = g \cdot (n \cdot x) = g \cdot x = (gN) \cdot x$$

が成り立つ．また，

(1) 任意の $gN, g'N \in G/N$ と任意の $x \in X$ に対して，

$$gN \cdot (g'N \cdot x) = gN \cdot (g' \cdot x) = g \cdot (g' \cdot x) = (gg') \cdot x = (gg'N) \cdot x$$

(2) 任意の $x \in X$ に対して，$N \cdot x = x$

となるので，G/N が X に作用することが分かる．このような G/N の X への作用を，G の作用から**誘導された作用** (induced action) という．

すなわちこれは，G の X への作用を与える写像 $\rho : G \times X \to X$ に対して，$(gN, x) \mapsto g \cdot x$ によって定まる，ρ から誘導された写像 $\overline{\rho} : G/N \times X \to X$ を考えることにほかならない．

今，N の作用は自明であるから，X の G-軌道分解と，G/N-軌道分解は一致する．すなわち，(5.1) において，任意の $\lambda \in \Lambda$ に対して，$(G/N)_{x_\lambda} = G_{x_\lambda}$ であり，X の G/N-軌道分解

$$X = \coprod_{\lambda \in \Lambda} (G/N)_{x_\lambda}$$

を得る．

最後に，群の作用のもう一つ別の見方について解説する．

定義 5.16 (置換群) X を空でない集合とする．X から X への全単射全体の集合を $\mathfrak{S}(X)$ とおくと，$\mathfrak{S}(X)$ は写像を合成を積として群になる．実際，単位元は恒等写像 $\mathrm{id}_X : X \to X$ であり，$\sigma \in \mathfrak{S}(X)$ に対して，σ の逆元は逆写像 σ^{-1} で与えられる．この $\mathfrak{S}(X)$ を X 上の**置換群** (permutation group) という．

自然数 $n \geq 1$ に対し，$X = \{1, 2, \ldots, n\}$ の場合，$\mathfrak{S}(X)$ は n 次対称群 $\mathfrak{S}_n$ にほかならない．

定義 5.17 (置換表現) G を群，X を空でない集合とする．一般に，G から $\mathfrak{S}(X)$ への群準同型写像を G の X 上の**置換表現** (permutation representation) という．特に，単射な置換表現を**忠実** (faithful) な置換表現という．

注意 5.18 群 G および空でない集合 X に対して，G の X への作用を与えることと，G の X 上の置換表現を与えることは同値である．実際，G が X に作用しているとき，写像 $f : G \to \mathfrak{S}(X)$ を

$$g \mapsto f_g := (x \mapsto g \cdot x, \quad x \in X)$$

によって定める．このとき，各 f_g は X 上の全単射であり，任意の $g,h \in G$ に対して，

$$f_{gh}(x) = (gh)\cdot x = g\cdot(h\cdot x) = f_g(f_h(x)) = (f_g \circ f_h)(x), \quad x \in X$$

となるから，f は準同型写像である．すなわち，f は G の X 上の置換表現である．

一方，G の X 上の置換表現 $f : G \to \mathfrak{S}(X)$ が与えられたとき，写像 $\rho : G \times X \to X$ を

$$(g,x) \mapsto f_g(x)$$

で定めると，任意の $g,h \in G$ と任意の $x \in X$ に対して，

$$\rho(g,\rho(h,x)) = \rho(g,f_h(x)) = f_g(f_h(x)) = f_{gh}(x) = \rho(gh,x)$$

が成り立つ．また，任意の $x \in X$ に対して，$\rho(1_G,x) = x$ となることも明らか．したがって，注意 5.2 により，G は X に作用する．

上の状況において，二つの操作が互いに他の逆の操作になっていることも簡単に確かめられる．よって，G の X への作用を与えることと，G の X 上の置換表現を与えることは同値である．したがって，群 G の X への作用がどれだけあるかを調べるには，置換表現 $G \to \mathfrak{S}(X)$ がどれだけあるかを調べればよいことが分かる．特に，自明な置換表現 $\mathrm{triv} : G \to \mathfrak{S}(X)$,

$$g \mapsto \mathrm{id}_X$$

に対応する作用が自明な作用である．

5.2 群の作用の例

ここでは，いくつかの具体的な例を通して群の作用を身近に捉えてみよう．

例 5.19 複素平面 $\mathbb{C}$ 内の単位円周

$$U := \{\exp(\theta\sqrt{-1}) \in \mathbb{C} \mid \theta \in \mathbb{R}\} \subset \mathbb{C}$$

を考え，複素数の通常の積により乗法群とみなす．このとき，U の $\mathbb{C}$ への作用を，任意の $\exp(\theta\sqrt{-1}) \in U$ と任意の $z \in \mathbb{C}$ に対して，

$$\exp(\theta\sqrt{-1}) \cdot z := \exp(\theta\sqrt{-1})z \quad （右辺は通常の複素数の積）$$

で定める．すなわち，$\exp(\theta\sqrt{-1})$ の z への作用は，z を原点を中心に時計回りに θ だけ回転させる作用である．すると，$z \in \mathbb{C}$ の軌道は，$\mathbb{C}$ 内の原点中心で半径 $|z|$ の円周である．特に，U の固定点は原点のみである．よって，$\mathbb{C}$ の U-軌道分解は

$$\mathbb{C} = \coprod_{x \in \mathbb{R}_{\geq 0}} U_x$$

となる．

例 5.20 自然数 $n \geq 1$ に対して，複素一般線型群 $\mathrm{GL}(n, \mathbb{C})$ および，n 次元複素ベクトル空間

$$\mathbb{C}^n := \left\{ \boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \middle| \, x_i \in \mathbb{C} \right\}$$

を考える．このとき，$\mathrm{GL}(n, \mathbb{C})$ の $\mathbb{C}^n$ への作用を，任意の $A \in \mathrm{GL}(n, \mathbb{C})$ と任意の $\boldsymbol{x} \in \mathbb{C}^n$ に対して，

$$A \cdot \boldsymbol{x} := A\boldsymbol{x} \quad （右辺は通常の複素数の積）$$

で定める．すると，零ベクトル $\mathbf{0}$ は明らかに $\mathrm{GL}(n, \mathbb{C})$-固定点であるから，$\{\mathbf{0}\}$ で一つの軌道である．一方，任意の $\boldsymbol{x} \neq \mathbf{0}$ に対して，$\boldsymbol{x}$ に $n-1$ 個のベクトルを付け足して $\mathbb{C}^n$ の基底を作ることができる．これを $(\boldsymbol{x}, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-1})$ とおく．このとき，$A = (\boldsymbol{x}\, \boldsymbol{x}_1 \, \cdots \, \boldsymbol{x}_{n-1})$ とおくと，A は $\mathbb{C}^n$ の標準基底 $(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n)$ を $(\boldsymbol{x}, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-1})$ に写す $\mathrm{GL}(n, \mathbb{C})$ の元である．特に，$A\boldsymbol{e}_1 = \boldsymbol{x}$ となる．ゆえに，$\boldsymbol{x} \neq \mathbf{0}$ なるベクトル $\boldsymbol{x}$ は $\boldsymbol{e}_1$ の軌道に属する．したがって，$\mathbb{C}^n$ の $\mathrm{GL}(n, \mathbb{C})$-軌道分解は

$$\mathbb{C}^n = \{\mathbf{0}\} \cup \mathrm{GL}(n, \mathbb{C})_{\boldsymbol{e}_1}$$

となる．

例 5.21 複素平面内の上半平面

$$\mathfrak{H} := \{z = x + y\sqrt{-1} \in \mathbb{C} \mid x, y \in \mathbb{R},\ y > 0\}$$

を考える[43]．$\mathrm{SL}(2,\mathbb{R})$ の $\mathfrak{H}$ への作用を，任意の $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R})$ と任意の $z \in \mathfrak{H}$ に対して，

$$A \cdot z := \frac{az+b}{cz+d}$$

によって定める．これが作用になっていることは次のようにして確かめられる．まず，

$$\frac{az+b}{cz+d} = \frac{1}{|cz+d|^2}(acz\overline{z} + bd + bc(z+\overline{z}) + (ad-bc)z)$$

より，

$$\mathrm{Im}(A \cdot z) = \frac{(ad-bc)\mathrm{Im}(z)}{|cz+d|^2} = \frac{\mathrm{Im}(z)}{|cz+d|^2}$$

となる．したがって，任意の $z \in \mathfrak{H}$, $A \in \mathrm{SL}(2,\mathbb{R})$ に対して，$A \cdot z \in \mathfrak{H}$ である．一方，単位行列 E_2 および任意の $z \in \mathfrak{H}$ に対して，$E_2 \cdot z = z$ となることは明らか．また，任意の $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ と任意の $z \in \mathfrak{H}$ に対して，

$$\begin{aligned} A \cdot (B \cdot z) &= A \cdot \left(\frac{rz+s}{tz+u}\right) = \frac{a\frac{rz+s}{tz+u} + b}{c\frac{rz+s}{tz+u} + d} = \frac{(ar+bt)z + as + bu}{(cr+dt)z + cs + du} \\ &= (AB) \cdot z \end{aligned}$$

となる．ゆえに，$\mathrm{SL}(2,\mathbb{R})$ は $\mathfrak{H}$ に作用する．

さて，次に $i = \sqrt{-1} \in \mathfrak{H}$ の固定化群について考察しよう．$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S_{\mathrm{SL}(2,\mathbb{Z})}(i)$ とすると，$A \cdot i = i$ なる条件から $d = a$, $c = -b$ を得る．すなわち，

$$S_{\mathrm{SL}(2,\mathbb{Z})}(i) = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R}) \mid a, b \in \mathbb{R},\ a^2 + b^2 = 1 \right\}$$

となる．この群は 2 次の**特殊直交群** (special orthonormal group)

[43] $\mathfrak{H}$ はドイツ装飾大文字の H．Half plane の頭文字である．

と呼ばれるものであり，通常 SO(2) と書かれる．

$\mathfrak{H}$ の部分集合

$$F := \{z = x + y\sqrt{-1} \in \mathfrak{H} \mid -\frac{1}{2} < x \leq \frac{1}{2},\ |z| > 1\}$$
$$\cup \{z = x + y\sqrt{-1} \in \mathfrak{H} \mid |z| = 1,\ x \geq 0\}$$

を考える．すると，F は $\mathrm{SL}(2, \mathbb{Z})\backslash\mathfrak{H}$ の完全代表系であり，

$$\mathfrak{H} = \coprod_{z \in F} (\mathrm{SL}(2, \mathbb{Z}))_z$$

と軌道分解されることが知られている[44]．

44) 高木貞治著『初等整数論講義』[6] を参照せよ．

5.3 半直積群

この節では，群の群への作用を利用して直積群の一般化である半直積群について考察する．応用として，正二面体群の一般化であって，メタ巡回群の一例となっているような群を解説する．シローの定理の証明には用いない事項であるので初学者は読み飛ばしても問題ない．

まず初めに，群の群への作用について考える．これは，以下に示すように群の集合への作用の定義において，さらに一つの条件を付け加えたものになっている．

定義 5.22（群の群への作用） G, H を群とする．任意の $g \in G$ と任意の $h \in H$ に対して，ある元 $g \cdot h \in H$ が定義されていて，

(1) 任意の $g, g' \in G$ と任意の $h \in H$ に対して，$g \cdot (g' \cdot h) = (gg') \cdot h$ が成り立つ．
(2) 任意の $h \in H$ に対して，$1_G \cdot x = x$.
(3) 任意の $g \in G$ と任意の $h, h' \in H$ に対して，$g \cdot (hh') = (g \cdot h)(g \cdot h')$ が成り立つ．

を満たすとき，G は H に（左から）**作用する**といい，$G \curvearrowright H$ と表す．

群の集合への作用の場合と同じように，**自明な作用**，**軌道**や**固定点**などの概念が定義できる（各自書き下してみよ）．

注意 5.23 群 G に対して，注意 5.11 で述べた G の共役作用は上の意味での作用にもなっている．実際，(3) の性質が成り立つことが次のようにして確かめられる．任意の $g, h, h' \in G$ に対して，

$$g \cdot (hh') = g(hh')g^{-1} = (ghg^{-1})(gh'g^{-1}) = (g \cdot h)(g \cdot h')$$

が成り立つ．

群の集合への作用は，その群の置換表現を考えることと同値であった．これに対応する概念を考えよう．そのために群の自己同型群なる概念を準備する．

定義 5.24（自己同型群） 群 G に対して，G から G への同型写像を G の**自己同型** (automorphism) という．G の自己同型写像全体を

$$\mathrm{Aut}(G) := \{\sigma : G \to G \,|\, \sigma \text{ は自己同型 }\}$$

とおく．このとき，$\mathrm{Aut}(G)$ は写像の合成に関して群をなす．単位元は $\mathrm{id}_G \in \mathrm{Aut}(G)$ であり，任意の $\sigma \in \mathrm{Aut}(G)$ の逆元は逆写像である．この群 $\mathrm{Aut}(G)$ を G の**自己同型群** (automorphism group) という．

ここで簡単な例を一つ考えよう．自然数 $n \geq 2$ に対して，加法的巡回群 $\mathbb{Z}/n\mathbb{Z}$ を考える．$\mathbb{Z}/n\mathbb{Z}$ には，自然に乗法が

$$[a]_n \cdot [b]_n := [ab]_n, \quad [a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$$

によって定義される（この積に関して $\mathbb{Z}/n\mathbb{Z}$ は乗法群にはならないことに注意せよ．実際，$[0]_n$ の逆元がない）．このとき，

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^\times &:= \{[m]_n \in \mathbb{Z}/n\mathbb{Z} \,|\, 0 \leq m \leq n-1,\ \gcd(m,n) = 1\} \\ &\subset \mathbb{Z}/n\mathbb{Z}\end{aligned}$$

を考える．ここで，$\gcd(m,n) = 1$ なる $m \in \mathbb{Z}$ に対して，$[m]_n$ に属する元はすべて n と互いに素であることに注意せよ．実際，任

意の $m' \in [m]_n$ に対して，剰余の定理よりある整数 k が存在して $m' = m + nk$ と書ける．もし $\gcd(m', n) = d > 1$ となったとすると $d|m$ かつ $d|n$ となるので矛盾．ゆえに $\gcd(m', n) = 1$ である．したがって，上の定義は well-defined である．

定理 5.25 以上の記号の下，

(1) $(\mathbb{Z}/n\mathbb{Z})^{\times}$ は $\mathbb{Z}/n\mathbb{Z}$ の乗法に関して位数 $\varphi(n)$ の乗法群になる．ここで，$\varphi(n)$ はオイラー関数を表す．この乗法群 $(\mathbb{Z}/n\mathbb{Z})^{\times}$ を法 n に関する**既約剰余類群** (group of reduced residue classes) という．

(2) $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^{\times}$.

証明. (1) まず，$\gcd(m, n) = \gcd(m', n) = 1$ なる任意の $[m]_n, [m']_n \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ に対して $\gcd(mm', n) = 1$ であるから，$[m]_n \cdot [m']_n = [mm']_n \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ となり，$(\mathbb{Z}/n\mathbb{Z})^{\times}$ は積について閉じている．この積に関して結合法則が成り立つことは，$\mathbb{Z}$ でそれが成り立つことから明らか．また，$[1]_n \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ である．一方，任意の $[m]_n \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ に対して $\gcd(m, n) = 1$ であるから，ある整数 $x, y \in \mathbb{Z}$ で，$mx + ny = 1$ となるものが存在する．このとき，$\gcd(x, n) = 1$ であり，$[x]_n = ([m]_n)^{-1} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ である．よって，$(\mathbb{Z}/n\mathbb{Z})^{\times}$ は群である．位数が $\varphi(n)$ になることは φ の定義から明らか．

(2) 任意の $\sigma \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ に対して，$\sigma([1]_n) = [m]_n = m[1]_n$ とおくと，σ は同型写像であるから $[m]_n$ は加法群 $\mathbb{Z}/n\mathbb{Z}$ の生成元でなければならない．もしそうでなければ，$\mathrm{Im}(\sigma) = \langle [m]_n \rangle \neq \mathbb{Z}/n\mathbb{Z}$ となり矛盾である．したがって，命題 2.36 より，$\gcd(m, n) = 1$ でなければならない．そこで，写像 $f : \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^{\times}$ を

$$\sigma \mapsto \sigma([1]_n)$$

で定める．このとき，f は同型写像である．実際，任意の $\sigma, \tau \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ に対して，$\sigma([1]_n) = [m]_n, \tau([1]_n) = [m']_n$ とするとき，

$$
\begin{aligned}
f(\sigma\tau) &= (\sigma\tau)([1]_n) = \sigma([m']_n) = \sigma(m'[1]_n) \\
&= m'\sigma([1]_n) = m'[m]_n \\
&= [mm']_n = [m]_n \cdot [m']_n = f(\sigma)f(\tau)
\end{aligned}
$$

となるので，f は準同型写像である．

f が全単射になることを示そう．$\sigma, \tau \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ に対して，$f(\sigma) = f(\tau)$ と仮定すると，$\sigma([1]_n) = \tau([1]_n)$ である．したがって，任意の $k \in \mathbb{Z}$ に対して，$\sigma([k]_n) = k\sigma([1]_n) = k\tau([1]_n) = \tau([k]_n)$ となり，$\sigma = \tau$ を得る．よって，f は単射である．一方，任意の $[m]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対して，写像 $\sigma : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ を $[k]_n \mapsto m[k]_n = [mk]_n$ で定める．すると，σ は $\mathbb{Z}/n\mathbb{Z}$ の同型写像である．実際，$[k]_n = [l]_n$ であれば $n|(mk-ml)$ であるから，$[mk]_n = [ml]_n$ となり，σ は well-defined．また，任意の $[k]_n, [l]_n \in \mathbb{Z}/n\mathbb{Z}$ に対して，

$$
\begin{aligned}
\sigma([k]_n + [l]_n) &= \sigma([k+l]_n) = [m(k+l)]_n \\
&= [mk]_n + [ml]_n = \sigma([k]_n) + \sigma([l]_n)
\end{aligned}
$$

であるから，σ は準同型写像である．任意の $[l]_n \in \mathbb{Z}/n\mathbb{Z}$ に対し，$\gcd(m,n) = 1$ より，$mx + ny = 1$ なる $x, y \in \mathbb{Z}$ が存在し，$mxl + nyl = l$ となる．よって，$\sigma([xl]_n) = [mxl]_n = [l]_n$ となるので σ は全射．さらに，$\sigma([k]_n) = \sigma([l]_n)$ と仮定すると，$[mk]_n = [ml]_n$ となるが，上で用いた x を両辺に乗じれば，$[k]_n = [l]_n$ となる．よって，σ は単射．

以上より，$\sigma \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ であることが分かる．このとき，$f(\sigma) = [m]_n$ であるから f は全射である．ゆえに，f は同型写像である．□

ここで，既約剰余類群の構造に関する定理を一つ挙げておく．

定理 5.26 $n_1, n_2, \ldots, n_r$ を互いに素な自然数とし，$n = n_1 n_2 \cdots n_r$ とおく．このとき，

$$
(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})^\times
$$

である．

証明. 帰納法を考えることにより，$r=2$ の場合に証明できればよい．中国式剰余定理（定理 3.30）の証明で用いた写像 $f:(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times$

$$[x]_n \mapsto ([x]_{n_1}, [x]_{n_2})$$

を考える．$\gcd(x,n)=1$ のとき，$\gcd(x,n_1)=\gcd(x,n_2)=1$ であることに注意して，f が well-defined であることが分かる．また，任意の $[x]_n, [y]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対して，

$$\begin{aligned} f([x]_n[y]_n) &= f([xy]_n) = ([xy]_{n_1}, [xy]_{n_2}) \\ &= ([x]_{n_1}, [x]_{n_2})([y]_{n_1}, [y]_{n_2}) = f([x]_n)f([y]_n) \end{aligned}$$

であるから f は準同型である．

一方，任意の $([x]_{n_1}, [y]_{n_2}) \in (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times$ をとる．$\gcd(n_1,n_2)=1$ であるから，$an_1+bn_2=1$ なる $a,b\in\mathbb{Z}$ が取れる．よって，$axn_1+bxn_2=x$ かつ $ayn_1+byn_2=y$ であり，$z=ayn_1+bxn_2\in\mathbb{Z}$ とおく．もし $\gcd(z,n)\neq 1$ だとすると，ある素数 p で z と n を割り切るものが存在する．したがって，p は n_1 または n_2 のどちらかを割り切る．$p|n_1$ とする．すると，$p|bxn_2$ となる．$p|b$ とすると $an_1+bn_2=1$ に矛盾するので $p \not| b$．また，$p|x$ とすると $\gcd(x,n)=1$ 矛盾するので $p \not| x$．したがって，$p|n_2$ となる．これは $\gcd(n_1,n_2)=1$ に矛盾．$p|n_2$ の場合も同様である．よって，$\gcd(z,n)=1$．このとき，

$$f([z]_n) = ([z]_{n_1}, [z]_{n_2}) = ([x]_{n_1}, [y]_{n_2})$$

となるので，f は全射である．f が単射であることは中国式剰余定理の場合と同様である．以上より，f は同型写像である．□

注意 5.27 この定理より，既約剰余類群 $(\mathbb{Z}/n\mathbb{Z})^\times$ の構造は，各素数 p に対して $(\mathbb{Z}/p^m\mathbb{Z})^\times$ の構造が分かればよいことが分かる．一般に次のことが知られている[45]．

(1) p を奇素数，$m\geq 1$ を自然数とするとき，$(\mathbb{Z}/p^m\mathbb{Z})^\times$ は巡回群 $\mathbb{Z}/p^{m-1}(p-1)\mathbb{Z}$ である．

(2) $(\mathbb{Z}/2^m\mathbb{Z})^\times$ は $m=1,2$ のとき巡回群 $\mathbb{Z}/2^{m-1}\mathbb{Z}$ であり，$m\geq 3$

45) 例えば，倉田令二朗著『平方剰余の相互法則』[3] などを参照されたい．

のときは $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$ に同型である．

定義 5.28（内部自己同型群） 群 G および，任意の $g \in G$ に対して，写像 $\theta_g : G \to G$ を

$$x \mapsto gxg^{-1}, \quad x \in G$$

で定めると，θ_g は G の自己同型になる．これを，g に付随する G の**内部自己同型** (inner automorphism) という．

G の内部自己同型写像全体を

$$\mathrm{Inn}(G) := \{\theta_g : G \to G \,|\, g \in G\}$$

とおく．このとき，$\mathrm{Inn}(G)$ は $\mathrm{Aut}(G)$ の部分群をなす．実際，$\mathrm{id}_G = \theta_{1_G}$ であり，任意の $g, h \in G$ に対して，$\theta_g\theta_h = \theta_{gh}$，$\theta_g^{-1} = \theta_{g^{-1}}$ となる．この部分群を，G の**内部自己同型群** (inner automorphism group) という．

命題 5.29 G を群とする．このとき，$G/Z(G) \cong \mathrm{Inn}(G)$ である．

証明. 写像 $f : G \to \mathrm{Inn}(G)$ を $g \mapsto \theta_g$ によって定める．すると，f は全射準同型写像である．実際，f の全射性は定義から明らかであり，任意の $g, h \in G$ および任意の $x \in G$ に対して，

$$\begin{aligned} f(gh)(x) &= (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} \\ &= g(\theta_h(x))g^{-1} = \theta_g(\theta_h(x)) = (f_g f_h)(x) \end{aligned}$$

となるので，$f(gh) = f(g)f(h)$ を得る．すなわち，f は準同型写像である．

次に，$\mathrm{Ker}(f) = Z(G)$ であることを確かめよう．これは，$g \in G$ に対して，

$$\begin{aligned} g \in \mathrm{Ker}(f) &\iff \theta_g = \mathrm{id}_G \\ &\iff gxg^{-1} = x, \quad x \in G \\ &\iff g \in Z(G) \end{aligned}$$

であることから直ちに従う．以上より，準同型定理から求める結果

を得る．□

さて，群 G が群 H に作用しているとする．各 $g \in G$ に対して，写像 $\sigma_g : H \to H$ を $h \mapsto g \cdot h$ によって定める．すると，$\sigma_g \in \mathrm{Aut}(H)$ である．実際，各 $g \in G$ に対して，作用の (3) の条件より，σ_g は準同型写像であることが分かる．さらに，$\sigma_g \sigma_{g^{-1}} = \sigma_{g^{-1}} \sigma = \mathrm{id}_H$ であるから，σ_g は全単射である．そこで，写像 $\sigma : G \to \mathrm{Aut}(H)$ を $g \mapsto \sigma_g$ によって定めると，作用の (1) の条件より，σ は準同型写像であることが分かる．

逆に，準同型写像 $\sigma : G \to \mathrm{Aut}(H)$ が与えられると，任意の $g \in G$ と任意の $h \in H$ に対して，

$$g \cdot h = \sigma_g(h)$$

と定めることで，G が H に作用することが分かる．以上の二つの操作は互いに他の逆の操作になっており，したがって，

G の H への作用を与える． $\iff$ 準同型写像 $G \to \mathrm{Aut}(H)$ を与える．

を得る．すなわち，群 G の群 H への作用がどれだけあるかを調べるには，準同型写像 $G \to \mathrm{Aut}(H)$ がどれだけあるかを調べればよいことが分かる．群の集合への作用の場合と同様に，自明な準同型 $\mathrm{triv} : G \to \mathrm{Aut}(H)$,

$$g \mapsto \mathrm{id}_H$$

に対応する G の H への作用が自明な作用である．

さて，群の半直積の概念を解説しよう．

定義 5.30（半直積群） K を群，$\sigma : K \to \mathrm{Aut}(H)$ を準同型写像とする．このとき，集合としての直積 $G := H \times K$ を考え，G に演算 $\cdot$ を任意の $(h, k), (h', k') \in G$ に対して，

$$(h, k) \cdot (h', k') := (h\sigma_k(h'), kk')$$

で定める．すなわち，K 成分のほうは通常の K の積で考え，H 成分の方は後ろの元 h' を k の作用で捻ってから掛け合わせるというも

のである．このとき，G はこの演算に関して群になる．実際，任意の $(h,k),(h',k'),(h'',k'') \in G$ に対して，

$$
\begin{aligned}
((h,k)\cdot(h',k'))\cdot(h'',k'') &= (h\sigma_k(h'),kk')\cdot(h'',k'') \\
&= ((h\sigma_k(h'))\sigma_{kk'}(h''),(kk')k'') \\
(h,k)\cdot((h',k')\cdot(h'',k'')) &= (h,k)\cdot(h'\sigma_{k'}(h''),k'k'') \\
&= (h\sigma_k(h'\sigma_{k'}(h'')),k(k'k''))
\end{aligned}
$$

であるので，σ が準同型であることと，H, K の結合法則から G の結合法則が従う．また，$(1_H,1_K) \in G$ なる元を考えると，任意の $(h,k) \in G$ に対して，

$$
\begin{aligned}
(1_H,1_K)\cdot(h,k) &= (\sigma_{1_K}(h),1_K k) = (h,k) \\
(h,k)\cdot(1_H,1_K) &= (h\sigma_k(1_H),k1_K) = (h,k)
\end{aligned}
$$

となるので，$(1_H,1_K)$ は G の単位元である．最後に，任意の $(h,k) \in G$ に対して，$(\sigma_k^{-1}(h^{-1}),k^{-1}) \in G$ なる元を考えると，

$$
\begin{aligned}
(h,k)\cdot(\sigma_k^{-1}(h^{-1}),k^{-1}) &= (h\sigma_k(\sigma_k^{-1}(h^{-1})),kk^{-1}) = (1_H,1_K) \\
(\sigma_k^{-1}(h^{-1}),k^{-1})\cdot(h,k) &= (\sigma_k^{-1}(h^{-1})\sigma_{k^{-1}}(h),k^{-1}k) = (1_H,1_K)
\end{aligned}
$$

となる（$\sigma_k^{-1} = \sigma_{k^{-1}}$ に注意せよ．）ので，$(h,k)^{-1} = (\sigma_k^{-1}(h^{-1}),k^{-1})$ である．

以上より，G は上の演算に関して乗法群をなす．これを H と K の**半直積群** (semidirect product group) [46] といい，$G = H \rtimes_\sigma K$ と書く．前後の文脈から，作用 σ が明らかなときは単に，$G = H \rtimes K$ とも書く．

46) 外部半直積とはあまりいわない．

注意 5.31 外部直積の場合と違って，半直積は H と K が積に関して対称的でない．特に，どちらがどちらに作用しているのを明示する必要がある．そのために，$\times$ ではなく $\rtimes$ なる記号を用いる．「閉じているほうの群が開いているほうの群に作用している」と覚えよう．

K の H への作用が自明なとき，すなわち，σ が自明な準同型のとき半直積は外部直積にほかならない．

命題 5.32 K を群，$\sigma : K \to \mathrm{Aut}(H)$ を準同型写像とし，$G =$

$H \rtimes_\sigma K$ とする．また，

$$\overline{H} := \{(h, 1_K) \in G \,|\, h \in H\}$$
$$\overline{K} := \{(1_H, k) \in G \,|\, k \in K\}$$

とおく．このとき，以下が成り立つ．

(1) $\overline{H}, \overline{K}$ はともに G の部分群であり，$\overline{H} \cong H, \overline{K} \cong K$.
(2) $G = \overline{H}\,\overline{K}$.
(3) $\overline{H} \lhd G$ で，$\overline{H} \cap \overline{K} = \{(1_H, 1_K)\}$.

証明. (1) 写像 $f_H : H \to \overline{H}$ を $h \mapsto (h, 1_K)$ によって定める．明らかに f_H は全射である．よって，f_H が単射準同型写像であることを示せば，$\mathrm{Im}(f_H) = \overline{H}$ は G の部分群で，かつ H と同型になることが示される．そこで，任意の $h, h' \in H$ に対して，

$$f_H(hh') = (hh', 1_K) = (h, 1_K)(h', 1_K) = f_H(h)f_H(h')$$

となるので f_H は準同型写像である．f_H が単射であることは定義から明らか．同様にして，$K \cong \overline{K} \leq G$ であることも示される．

(2) $\supset$ の包含関係は明らかゆえ，$\subset$ を示せばよい．ところが，任意の $(h, k) \in G$ に対して，$(h, 1_K)(1_H, k) = (h, k) \in \overline{H}\,\overline{K}$ ゆえ，これより直ちに従う．

(3) 任意の $(h, 1_K) \in \overline{H}$ および任意の $(h', k') \in G$ に対して，

$$\begin{aligned}(h', k')(h, 1_K)(h', k')^{-1} &= (h'\sigma_{k'}(h), k')(\sigma_{k'}^{-1}((h')^{-1}), (k')^{-1}) \\ &= (h'\sigma_{k'}(h)(h')^{-1}, 1_K) \in \overline{H}\end{aligned}$$

となるので，$\overline{H} \lhd G$ である．一方，$\overline{H} \cap \overline{K} = \{(1_H, 1_K)\}$ であることは明らか．□

次に，内部直積の一般化である内部半直積について考えよう．つまり，ある群 G の中に二つの部分群 H, K があって G がそれらの半直積と同型になる場合について考える．

定義 5.33（内部半直積） G を群，H, K を部分群とする．さらに，

$$G = HK, \quad H \lhd G, \quad H \cap K = \{1_G\}$$

となっているとする．このとき，G を H と K の**内部半直積** (interior semidirect product) といい，$G = H \dot{\rtimes} K$ と表す．

以下に示すように，内部半直積 $G = H \dot{\rtimes} K$ は K の H への共役作用に関する半直積とみなせる．

命題 5.34 内部半直積として表された群 $G = H \dot{\rtimes} K$ を考える．

(1) 各 $k \in K \subset G$ に対して，k に付随する G の内部自己同型 $\theta_k \in \mathrm{Inn}(G)$ を H に制限したもの $\theta_k|_H : H \to H$ は H の自己同型である．このとき，写像 $\sigma : K \to \mathrm{Aut}(H)$ を $k \mapsto \theta_k|_H$ で定めると，σ は準同型写像である．

(2) $G \cong H \rtimes_\sigma K$.

証明. (1) 任意の $k \in K$ に対して，H は正規部分群であるから，$\mathrm{Im}(\theta_k|_H) \subset H$ である．また，$\theta_k|_H\, \theta_{k^{-1}}|_H = \theta_{k^{-1}}|_H\, \theta_k|_H = \mathrm{id}_H$ であるから，$\theta_k|_H \in \mathrm{Aut}(H)$ である．さらに，任意の $k, k' \in K$ および，任意の $h \in H$ に対して，

$$\theta_{kk'}|_H(h) = kk'h(k')^{-1}k^{-1} = \theta_k|_H(\theta_{k'}|_H(h)) = (\theta_k|_H\, \theta_{k'}|_H)(h)$$

となるので，σ は準同型写像である．

(2) 写像 $f : H \rtimes_\sigma K \to G$ を $(h, k) \mapsto hk$ によって定める．これが同型写像になることを示す．まず，任意の $(h, k), (h', k') \in H \rtimes_\sigma K$ に対して，

$$\begin{aligned} f((h,k)(h',k')) &= f((h\sigma_k(h'), kk')) = h\sigma_k(h')kk' = h(kh'k^{-1})kk' \\ &= hkh'k' = f((h,k))f((h',k')) \end{aligned}$$

となるので，f は準同型写像である．また，内部半直積の定義より $G = HK$ であるので f は明らかに全射である．さらに，$(h, k), (h', k') \in H \rtimes_\sigma K$ に対して，$f((h, k)) = f((h', k'))$ と仮定する．すると，$hk = h'k'$ より $(h')^{-1}h = k'k^{-1} \in H \cap K = \{1\}$ となるので，$h = h'$, $k = k'$ を得る．すなわち，f は単射である．以上より，f は同型写像である．□

系 5.35 内部半直積として表された群 $G = H \dot{\rtimes} K$ において，各

$g \in G$ に対して一意的にある $h \in H$, $k \in K$ が存在して，$g = hk$ と書ける．特に，$|G| < \infty$ のとき，$|G| = |H||K|$ が成り立つ．

証明. 前半は，命題 5.34 の (2) で考えた写像 f の単射性から直ちに従う．後半は前半より導かれる．□

さて，正二面体群の一般化を考えよう．

例 5.36 m, n を自然数とし，位数 m の加法的巡回群と位数 n の乗法的巡回群

$$H := \mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, \ldots, [m-1]_m\},$$
$$K := \langle\, t \,\rangle = \{1, t, \ldots, t^{n-1}\}$$

を考える．今，準同型写像 $\sigma : K \to \mathrm{Aut}(H) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}$ が与えられているとする．σ の像は $\sigma_t := \sigma(t)$ の値によって完全に決まる．そこで，σ_t を

$$[1]_m \mapsto [r]_m$$

なる H 上の同型写像とする．すなわち，任意の $j \in \mathbb{Z}$ に対して $\sigma_t([j]_m) = [rj]_m$，および σ_{t^i} は

$$[j]_m \mapsto r^i[j]_m = [r^i j]_m, \quad 0 \leq j \leq m-1$$

を満たすとする．このとき，

$$G_{m,n}(r) := H \rtimes_{\sigma} K$$

とおく．このとき，$|G_{m,n}(r)| = mn$. また，σ が自明な準同型（$\mathrm{Im}(\sigma) = \{\mathrm{id}_H\}$ なる準同型）でなければ，$r \not\equiv 1 \pmod{m}$ となり，$G_{m,n}(r)$ は非可換群である．実際，

$$([1]_m, 1_K)([0]_m, t) = ([1]_m + \sigma_{1_K}([0]_m), t) = ([1]_m, t)$$
$$([0]_m, t)([1]_m, 1_K) = ([0]_m + \sigma_t([1]_m), t) = ([r]_m, t)$$

である．さらに，

$$\begin{aligned}([0]_m, t)([1]_m, 1_K)([0]_m, t)^{-1} &= ([r]_m, t)(\sigma_t^{-1}([0]_m), t^{-1}) \\ &= ([r]_m, 1_K)\end{aligned}$$

が成り立つ．そこで，$a := ([1]_m, 1_K)$, $b := ([0]_m, t)$ とおくと，

$$G_{m,n}(r) = \{a^j b^i \,|\, 0 \leq j \leq m-1,\ 0 \leq i \leq n-1\}$$

と表され，

$$a^m = b^n = 1,\ bab^{-1} = \sigma^r,\ (\text{ただし，} r^n \equiv 1 \pmod{m}.)$$

を満たすことが分かる．

特に，$n = 2$ のとき，$-1 \in (\mathbb{Z}/m\mathbb{Z})^\times$ であり，$r = -1$ として $\sigma_t([1]_m) = [-1]_m$ なる準同型 $\sigma : K \to \mathrm{Aut}(H)$ を考えることができる．このとき，$G_{m,2}(-1)$ は m 次の正二面体群 D_m にほかならない．

定義 5.37（メタ巡回群） 群 G において，ある正規部分群 N であって，N と G/N がともに巡回群となるものを**メタ巡回群** (metacyclic group) という．

例 5.38 m, n を自然数とする．このとき，$G_{m,n}(r)$ はメタ巡回群である．実際，$G_{m,n}$ は位数 m の正規部分群である巡回群 H を持ち，H による G の剰余群 G/H は位数 n の巡回群である．

5.4 問題

問題 5.1 例 5.19 の作用を考える．自然数 $n \geq 2$ に対して，U の部分群である $\mathcal{U}_n$ の，$\mathbb{C}$ への作用を考える．このとき，$\mathbb{C}$ の $\mathcal{U}_n$-軌道分解を求めよ．

解答． まず，原点は固定点である．一方，任意の $z \in \mathbb{Z} \setminus \{0\}$ に対して，z の $\mathcal{U}_n$-軌道は

$$(\mathcal{U}_n)_z = \left\{ z \exp\left(\frac{2k\pi\sqrt{-1}}{n}\right) \in \mathbb{C} \,\middle|\, 0 \leq k \leq n-1 \right\}$$

であり，

$$F := \{z = r\exp(\theta\sqrt{-1}) \,|\, r \geq 0,\ 0 \leq \theta < \frac{2\pi}{n}\}$$

とおくと，

$$\mathbb{C} = \coprod_{z \in F} (\mathcal{U}_n)_z$$

が求める軌道分解である．□

問題 5.2 例 5.21 で考察した，$\mathrm{SL}(2,\mathbb{R})$ の $\mathfrak{H}$ への作用を考える．このとき，$\mathfrak{H}$ には固定点が存在しないことを示せ．

解答． $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R})$ なる元を考えると，任意の $z \in \mathfrak{H}$ に対して，$A \cdot z = z + 1$ となるので，A で固定されるような元は $\mathfrak{H}$ には存在しない．□

問題 5.3 m, n を自然数とし，例 5.36 の記号を踏襲してメタ巡回群 $G_{m,n}(r)$ を考える．このとき，以下を示せ．

(1) $[G_{m,n}(r), G_{m,n}(r)] = \langle ((r^i - 1)[1]_m, 1_K) \mid 0 \leq i \leq n-1 \rangle$.
(2) $G_{m,n}(r)^{\mathrm{ab}} \cong (H/\langle (r^i - 1)[1]_m \mid 0 \leq i \leq n-1 \rangle) \times K$.
(3) $n \geq 3$ のとき，$G_{m,n}(r)$ は任意の正二面体群と同型にはならない．
(4) m が素数のとき，

$$G_{m,n}(r)^{\mathrm{ab}} \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, & r \equiv 1 \pmod{m}, \\ \mathbb{Z}/n\mathbb{Z}, & r \not\equiv 1 \pmod{m}. \end{cases}$$

解答． (1) $[G_{m,n}(r), G_{m,n}(r)]$ は交換子

$$\begin{aligned} [([j]_m, t^i), ([j']_m, t^{i'})] &= ([j]_m, t^i)([j']_m, t^{i'})(\sigma_{t^i}^{-1}([-j]_m), t^{-i}) \\ &\quad (\sigma_{t^{i'}}^{-1}([-j']_m), t^{-i'}) \\ &= ([j]_m + \sigma_{t^i}([j']_m), t^{i+i'})(\sigma_{t^i}^{-1}([-j]_m) \\ &\quad + \sigma_{t^{-i}}(\sigma_{t^{i'}}^{-1}([-j']_m)), t^{-i-i'}) \\ &= ([j]_m + \sigma_{t^i}([j']_m) - \sigma_{t^{i'}}([j]_m) - [j']_m, 1_K) \\ &= ((1 - r^{i'})[j]_m + (r^i - 1)[j']_m, 1_K) \end{aligned}$$

たちで生成されているので，$[G_{m,n}(r), G_{m,n}(r)] \subset$ 右辺 となる．一方，右辺の生成元に関して

$$(r^i - 1)[1]_m = [([0]_m, t^i), ([1]_m, 1_K)] \in [G_{m,n}(r), G_{m,n}(r)]$$

であるので，逆向きの包含関係も従う．

(2) 右辺の群を W とおく．写像 $f : G_{m,n}(r) \to W$ を $([j]_m, t^i) \mapsto (\{[j]_m\}, t^i)$ で定めると f は全射準同型になる．（ここで，$\{z\}$ は $z \in H$ の属する剰余類を表す）実際，全射性は定義から明らかであり，

$$\begin{aligned} f(([j]_m, t^i)([j']_m, t^{i'})) &= f(([j + r^i j']_m, t^{i+i'})) \\ &= (\{[j + r^i j']_m\}, t^{i+i'}) \\ &= (\{[j + j']_m\}, t^{i+i'}) = (\{[j]_m\}, t^i)(\{[j']_m\}, t^{i'}) \\ &= f(([j]_m, t^i))f(([j']_m, t^{i'})) \end{aligned}$$

より f が準同型写像であることも分かる．よって，f は全射準同型写像 $\overline{f} : G_{m,n}(r)^{\mathrm{ab}} \to W$ を誘導する．

ここで，$q = |[G_{m,n}(r), G_{m,n}(r)]|$ とおくと，$|G_{m,n}(r)^{\mathrm{ab}}| = \frac{mn}{q}$，$|W| = \frac{m}{q}n$ であるから，$|G_{m,n}(r)^{\mathrm{ab}}| = |W|$．よって，$\overline{f}$ は単射である．したがって同型写像となり，求める結果を得る．

(3) (2) より，$G_{m,n}(r)$ のアーベル化には位数 n の元が含まれる．ところが，正二面体群のアーベル化は $\mathbb{Z}/2\mathbb{Z}$ か $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ のどちらかに同型であり，どちらにしても各元の位数は高々 2 である．よって，アーベル化したものが同型でないので，$G_{m,n}(r)$ は任意の正二面体群と同型ではない．

(4) $r \equiv 1 \pmod m$ のときは明らか．$r \not\equiv 1 \pmod m$ とすると，$r - 1 \not\equiv 0 \pmod m$ であるから，$\langle (r^i - 1)[1]_m \mid 0 \le i \le n-1 \rangle$ は $\mathbb{Z}/m\mathbb{Z}$ の非自明な部分群である．ところが，m は素数であるから，$\langle (r^i - 1)[1]_m \mid 0 \le i \le n-1 \rangle = \mathbb{Z}/m\mathbb{Z}$ でなければならない．これより求める結果を得る．□

問題 5.4 (1) 合同方程式 $x^3 \equiv 1 \pmod 7$ の解を求めよ．
(2) (1) で求めた x に対して，$G_{7,3}(x)^{\mathrm{ab}}$ を計算せよ．

解答. (1) $0 \le x \le 6$ に対して x^3 を計算することにより，$x \equiv 1, 2, 4 \pmod 7$ であることが分かる．

(2) 前問の (4) より，

$$G_{7,3}(x)^{\mathrm{ab}} \cong \begin{cases} \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, & x \equiv 1 \pmod 7 \\ \mathbb{Z}/3\mathbb{Z}, & x \equiv 2, 4 \pmod 7 \end{cases}$$

を得る.

6 シローの定理

以下，特に断らない限り， p は素数を表すものとする．本章の主な目標は，シローの定理の証明である．シローの定理の証明法はいくつか知られているが，ここでは **Wielandt** による証明を解説する．まず初めに， p 群に関するいくつかの性質をまとめておく．後半に，有限群の同型類決定問題への応用に関していくつか具体例を述べる．

6.1 p 群

定義 6.1（p 群）位数が素数 p の冪であるような非自明な群を p 群 (p-group) という．

命題 6.2 G を p 群とするとき，G の任意の部分群，および剰余群は p 群である．

証明. ラグランジュの定理より明らかである．□

ここで，一つ p 群に関する重要な定理を述べる．

定理 6.3 G を p 群とすると，G の中心は非自明である．すなわち，$Z(G) \neq \{1_G\}$ である．

証明. G の類等式 $|G| = |Z(G)| + l_1 + \cdots + l_s$ を考える．今，$p||G|$ であり，定理 4.4 より，各 $1 \leq i \leq s$ に対して $p|l_i$ である．したがって，$p||Z(G)|$ となり，$Z(G) \neq \{1_G\}$ であることが分かる．□

命題 6.4 G を，$|G| = p^2$ なる p 群とする．このとき，G はアーベル群である．

証明. p 群の中心は非自明な部分群であるから，$Z(G)$ の位数として考えられるのは p または p^2 である．もし，$|Z(G)| = p^2$ であれば，$G = Z(G)$ となり明らかに G はアーベル群となる．そこで，$|Z(G)| = p$ となったと仮定する．このとき，$G \neq Z(G)$ なので，ある $x \in G \setminus Z(G)$ が存在する．このとき，

$$\{1_G\} \subset Z(G) \subset \langle Z(G), x\rangle \subset C_x(G) \subset G$$

なる部分群の増大列が得られる．ところが，部分群の位数は p^2 の約数で，$|Z(G)| = p$ であるから，$|\langle Z(G), x\rangle| = p^2$，すなわち，$\langle Z(G), x\rangle = C_x(G) = G$ とならなければならない．特に，$C_x(G) = G$ は $x \in Z(G)$ を意味するが，これは矛盾である．よって，$|Z(G)| = p$ となることはない．以上より，求める結果を得る．
□

注意 6.5 命題 6.4 より，素数 $p > 1$ に対して，位数が p^2 の群は，$\mathbb{Z}/p^2\mathbb{Z}$ か $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ のどちらかに同型であることが分かる．

6.2 シローの定理の証明

定理 6.6（シローの定理） G を有限群，p を素数とする．このとき，以下が成り立つ．

(1) $m \in \mathbb{N}$ に対して，$p^m||G|$ であれば，G は位数 p^m の部分群を持つ．特に，p^n を $|G|$ を割る p の最大冪とすると，G は位数 p^n の部分群を持つ．これを，G の **p-シロー部分群** (p-Sylow subgroup) という．（p-シロー部分群は一般に一意的とは限らない．）
(2) G の任意の部分群で p 群であるものは，G のある p-シロー部分群に含まれる．
(3) G の p-シロー部分群はどの二つも共役である．
(4) G の p-シロー部分群の個数は $|G|$ の約数であり，$1 + pk$ なる形で表される．

証明. (1) $|G| = p^m d$ とし，d を割り切る p の最大冪を p^r $(r \geq 0)$ とおく．また，

$$X := \{A \subset G \,|\, A \text{ は } |A| = p^m \text{ なる } G \text{ の部分集合}\}$$

とおく．$|X|$ は $|G|$ 個の中から相異なる p^m 個の元を選ぶときの場合の数に等しいので，$|X| = \binom{p^m d}{p^m}$．このとき，$|X|$ を割り切る p の最大冪は p^r である．これを示すには，

$$|X| = \binom{p^m d}{p^m} = \frac{p^m d(p^m d - 1)(p^m d - 2)\cdots(p^m d - p^m + 1)}{p^m(p^m - 1)(p^m - 2)\cdots(p^m - p^m + 1)}$$

であるから，任意の $1 \leq i \leq p^m - 1$ に対して，$p^m d - i$ を割り切る p の最大冪と $p^m - i$ を割り切る p の最大冪が等しいことを示せばよい．すると，各 $1 \leq i \leq p^m - 1$ に対して，i を割り切る p の最大冪を p^l とすれば，$p^l < p^m$ であり，このとき，$p^l | (p^m d - i)$ かつ $p^l | (p^m - i)$ である．また，明らかに $p^{l+1} \nmid (p^m d - i)$ かつ $p^{l+1} \nmid (p^m - i)$ でもあるので，$p^m d - i$ および，$p^m - i$ を割り切る p の最大冪はともに p^l である．よって，$|X|$ を割り切る p の最大冪は d のそれに等しい．

次に，G の X への作用を，任意の $g \in G$ および，任意の $A \in X$ に対して，$g \cdot A := gA$ によって定める．X の G-軌道分解 $X = G_{A_1} \cup G_{A_2} \cup \cdots \cup G_{A_s}$ において，$p^{r+1} \nmid |X|$ であるから，$p^{r+1} \nmid |G_{A_i}|$ となる $1 \leq i \leq s$ が存在する．以下，この i を固定する．$|G_{A_i}| = k$ とおく．このとき，$|S_G(A_i)| = p^m$ である．実際，これは以下のようにして示される．まず，定理 5.7 より，$|G|/|S_G(A_i)| = |G_{A_i}| = k$ となるので，$|G| = p^m d = k|S_G(A_i)|$ を得る．今，$k|S_G(A_i)|$ を割り切る p の最大冪は p^{m+r} であり，$p^{r+1} \nmid k$ ゆえ $p^m \,|\, |S_G(A_i)|$ でなければならない．よって，$p^m \leq |S_G(A_i)|$ となる．一方，任意の $x \in A_i$ に対して，写像 $\rho_x : S_G(A_i) \to A_i$ を $h \mapsto hx$ で定める．$h, h' \in S_G(A_i)$ に対して，$hx = h'x$ とすれば，$h = h'$ となるので，ρ_x は単射である．よって，$|S_G(A_i)| \leq |A_i| \leq p^m$ となる．したがって，$|S_G(A_i)| = p^m$ となる．

(2) $|G| = p^e s$, $\gcd(p, s) = 1$ とし，P を G の一つの p-シロー部分群とする．$C(P)$ を G における P の共役部分群全体とすれば，定理 4.5 より，$|C(P)| = |G/N_P(G)|$ であるから，$|C(P)|$ は G の約数である．また，$P \leq N_P(G)$ であるから，$|N_P(G)| = |P|l$ なる

$l \in \mathbb{N}$がとれる．すると，

$$|C(P)| = |G|/|N_P(G)| = |G|/|P|l$$

より，$|C(P)|$ は $|G/P|$ の約数であり，したがって s の約数である．よって，$\gcd(|C(P)|, p) = 1$ である．

さて, H を G の任意の部分群で p 群であるものとする．G は $C(P)$ に共役により作用しているが，これを H に制限し軌道分解したものを

$$C(P) = C_{P_1} \cup C_{P_2} \cup \cdots \cup C_{P_t}$$

とする．$l_i := |C_{P_i}|$ とすると, 定理 4.5 より, $l_i = |H/(H \cap N_G(P_i))|$ となり，l_i は $|H|$ の約数である．特に，l_i は p の冪乗である．ところが, 上の議論より $\gcd(|C(P)|, p) = 1$ であるから，ある $1 \leq i \leq t$ で，$l_i = p^0 = 1$ となるものが存在する．このとき，$C_{P_i} = \{P_i\}$ であり，P_i は H の共役作用における固定点である．したがって，$H \leq N_{P_i}(G)$．また，明らかに，$P_i \lhd N_{P_i}(G)$ であるから，第 2 同型定理を用いて

$$HP_i/P_i \cong H/(H \cap P_i)$$

を得る．これより，$|HP_i/P_i| = |H/(H \cap P_i)|$ となる．ところが，各 P_i は P の共役部分群ゆえ $|P_i| = |P| = p^e$ であることに注意すると，$s = |G/P| = |G/P_i| = |G/HP_i||HP_i/P_i|$ より，$|HP_i/P_i|$ は s の約数である．一方，$|H/(H \cap P_i)|$ は $|H|$ の約数だから p の冪乗である．今，$\gcd(p, s) = 1$ であるから，

$$|HP_i/P_i| = |H/(H \cap P_i)| = 1$$

でなければならないことがわかる．よって，$H = H \cap P_i$，特に $H \subset P_i$ を得る．

(3) P, P' を G の二つの p-シロー部分群とする．$H = P'$ として (2) で用いた議論を適用すると，P' は P のある共役部分群 P'' に含まれることが分かる．ところが，P' も P'' も同じ位数 $|P|$ であるから，両者は一致しなければならない．つまり，$P' = P''$ は P の共役部分群である．

(4) P を G の一つの p-シロー部分群とする．定理 4.5 より，

$|C(P)| = |G/N_P(G)|$ は $|G|$ の約数である．一方，$H = P$ として (2) の議論を適用すると，$C(P)$ の P-軌道分解

$$C(P) = C_{P_1} \cup C_{P_2} \cup \cdots \cup C_{P_t}$$

を得る．今，$P \in C(P)$ であるから，ある $1 \leq i \leq t$ が存在して，$P \in C_{P_i}$ となる．ところが，P の P の元による共役部分群は明らかに P 自身であるから，$P_i = P$ であり，$C_{P_i} = C_P = \{P\}$ でなければならない．次に，$j \neq i$ なる $1 \leq j \leq t$ に対して，$|C_{P_j}| \neq 1$ である．もし，$|C_{P_j}| = 1$ とすると，$C_{P_j} = \{P_j\}$ となる．すると，$H = P$ として (2) で用いた議論を思い出すと，$P \subset P_j$ とならなければならない．特に，両者の位数を比べて，$P = P_j$ となるが，これは $j \neq i$ より矛盾である．よって，各 $|C_{P_j}|$ は 1 より真に大きい p の倍数である．したがって，$|C(P)|$ は $1 + pk$ なる形になる．□

命題 6.7 G を有限群とし，$p \,|\, |G|$ とする．G の p-シロー部分群がただ一つであれば，それは G の正規部分群である．

証明. P を G のただ一つの正規部分群とする．任意の $g \in G$ に対して，gPg^{-1} は P と共役な p-シロー部分群である．仮定により，$gPg^{-1} = P$ となるので P は G の正規部分群である．□

さて，具体的な例を通してシローの定理を確かめてみよう．

例題 6.8 3 次対称群 $\mathfrak{S}_3$ のシロー部分群をすべて求めよ．

解答. $|\mathfrak{S}_3| = 6 = 2 \cdot 3$ であるから，$\mathfrak{S}_3$ は位数 2 の 2-シロー部分群 P_2 と，位数 3 の 3-シロー部分群 P_3 を持つ．3-シロー部分群の個数 l は $l = 1 + 3n$ なる形をしているが，これが 6 の約数となるのは $l = 1$ の場合のみである．すなわち，3-シロー部分群の個数は 1 である．よって，P_3 は $\mathfrak{S}_3$ の正規部分群.

次に，2-シロー部分群について考える．その個数 k は $k = 1 + 2m$ なる形をしている．これが 6 の約数になるのは $k = 1, 3$ である．そこで，$k = 1$ と仮定する．このとき，2-シロー部分群 P_2 はただ一つであり，したがって正規部分群になる．P_2 および P_3 は素数位数の巡回群であり，それらの生成元をそれぞれ a, b とおくと，$ab = ba$ が成り立つ．実際，P_2 は正規部分群ゆえ，$bP_2b^{-1} = P_2$．したがっ

て，$bab^{-1} \in P_2$ となるが，もし $bab^{-1}=1$ とすると $a=1$ となるので矛盾．よって，$bab^{-1}=a$，すなわち，$ba=ab$ である．さて，$\mathfrak{S}_3$ において，a と b で生成される部分群を H とおくと，上の考察から H はアーベル群である．よって，補題 2.39 より，ab の位数は 6 となる．よって，$H=\mathfrak{S}_3 \cong \mathbb{Z}/6\mathbb{Z}$ となるが，$\mathfrak{S}_3$ は非可換群だからこれは矛盾．よって，$\mathfrak{S}_3$ の 2-シロー部分群は全部で 3 個ある．特に，これらは互換で生成される部分群である．

具体的にすべて求めると，3-シロー部分群は $P_3=\{1,(123),(132)\}$ であり，2-シロー部分群は

$$P_2=\{1,(12)\},\ \{1,(13)\},\ \{1,(23)\}$$

となる．□

6.3 シローの定理の適用例，および応用例

ここでは，シローの定理を適用して得られる諸性質や，群の同型類を決定する問題への応用例についていくつか解説する．これらの例を通して，シローの定理をより深く理解し，使いこなせるようになるのが目標である．

6.3.1 有限群に関する性質など

命題 6.9（コーシーの定理）G を有限群とし，$p \mid |G|$ とする．このとき，G は位数 p の元を持つ．

証明. シローの定理より，G は位数 p の部分群をもつ．位数 p の部分群は巡回群ゆえ，その生成元の位数は p となる．□

命題 6.10 G を有限群とし，$p \mid |G|$ とする．N を G の正規部分群とする．このとき，$\gcd(|G/N|,p)=1$ であれば，N は G のすべての p-シロー部分群を含む．

証明. P を G の p-シロー部分群とする．もし，$P \not\subset N$ とすると，ある $x \in P$ で $x \notin N$ となるものが存在する．x の G における位数を m とすると，$m \mid |P|$ より，m は p の冪乗の形をしている．一方，xN

の G/N における位数を n とする．このとき，$(xN)^m = x^m N = N$ となるので，$n|m$ である．つまり，n は p の冪乗の形をしている．ところが，$|G/N|$ は p と互いに素であるから，n は p の倍数ではない．したがって，$n = p^0 = 1$ でなければならない．つまり，$xN = N$ となるが，これは矛盾．したがって，$P \subset N$ である．□

命題 6.11 G を有限群とし，$|G| = p^e m$ とする．ここで，p は素数で，$\gcd(p, m) = 1$ である．$p > m$ のとき，G は正規部分群である p-シロー部分群を持つ．

証明. G の p-シロー部分群の個数は $1 + pk$ なる形をしている，$|G| = p^e m$ の約数である．ところが，$1 + pk$ は p と互いに素であるから，$1 + pk$ は m の約数でなければならない．ところが，$m < p$ であるから $1 + pk$ が m の約数となるには $k = 0$ しかない．すなわち，G の p-シロー部分群はただ一つである．よって，正規部分群となる．□

命題 6.12 G を有限群とし，N を G の正規部分群とし，P を N のある p-シロー部分群で正規部分群であるものとする．このとき，P は G の正規部分群である．

証明. 任意の $g \in G$ に対して，$gPg^{-1} \subset gNg^{-1} \subset N$ となる．よって，gPg^{-1} は位数が $|gPg^{-1}| = |P|$ なる N の部分群となるが，仮定により，N の p-シロー部分群はただ一つであるので，$gPg^{-1} = P$ である．つまり，P は G の正規部分群である．□

命題 6.13 G を有限群とし，P を G のある p-シロー部分群とする．N を $N_G(P) \subset N$ なる G の部分群とする．このとき，$N_G(N) = N$ である．

証明. $N_G(N) \subset N$ を示せばよい．任意の $g \in N_G(N)$ に対して，$gPg^{-1} \subset gN_G(P)g^{-1} \subset gNg^{-1} \subset N$ が成り立つ．すると，$|gPg^{-1}| = |P|$ であるから，P と gPg^{-1} はともに N の p-シロー部分群にもなっている．よって，これらは N において共役であるから，ある $x \in N$ が存在して $xPx^{-1} = gPg^{-1}$ となる．したがって，$P = (x^{-1}g)P(x^{-1}g)^{-1}$ となり，$x^{-1}g \in N_G(P) \subset N$ を得る．

よって，$g \in xN = N$ となり，求める結果を得る．□

命題 6.14 G を有限群とし，P を G のある p-シロー部分群とする．N を G の正規部分群とし，$P \cap N$ は自明な群ではないとする．このとき，$P \cap N$ は N の p-シロー部分群である．

証明. まず，$P \cap N \subset P$ であるから，$P \cap N$ は p-群である．一方，第 2 同型定理より，$|N/(N \cap P)| = |NP/P|$ であるが，$|NP/P| = |NP|/|P|$ であり，P が G に含まれる位数 p 冪の群で最大のものであることを考えると，$|NP/P|$ の素因数分解には p が現れない．したがって，$|N/(N \cap P)| = |N|/|(N \cap P)|$ の素因数分解に p が現れないことが分かり，$N \cap P$ は N に含まれる p 群のうち最大のものである．すなわち，$N \cap P$ は N の p-シロー部分群である．□

命題 6.15 G を有限群とし，P を G のある p-シロー部分群とする．N を G の正規部分群とする．このとき，$N_G(P) \subset N_G(N \cap P)$ が成り立つ．

証明. 任意の $g \in N_G(P)$ に対して，$g(N \cap P)g^{-1} = (gNg^{-1}) \cap (gPg^{-1}) = N \cap P$ となる．よって，$g \in N_G(N \cap P)$ である．□

命題 6.16 G を有限群とし，P を G のある p-シロー部分群とする．N を G の正規部分群とし，剰余群 PN/N は非自明とする．このとき，PN/N は G/N の p-シロー部分群である．

証明. 第 2 同型定理より，$|PN/N| = |P/(P \cap N)|$ である．よって，$|PN/N|$ は p の冪であり，PN/N は p-群である．今，第 3 同型定理より，$[G/N : PN/N] = [G : PN]$ であるが，$P \subset PN \subset G$ より，$[G : PN] = |G/PN|$ の素因数分解に p は現れない．したがって，$[G/N : PN/N]$ の素因数分解にも p は現れず，PN/N は G/N に含まれる位数が p 冪の部分群で最大のもであることが分かる．これより求める結果を得る．□

命題 6.17 有限アーベル群 G のすべての p-シロー部分群が巡回群であれば G は巡回群である．

証明. $|G|$ の素因数分解を $|G| = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ とする．各 $1 \leq i \leq r$ に対して P_i を位数 $p_i^{e_i}$ の部分群とすれば，有限アーベル群の構造定理より，

$$G \cong P_1 \times \cdots \times P_r$$

である．すなわち，G は p_i-シロー部分群 P_i たちの内部直積である．仮定により，各 P_i は位数 $p_i^{e_i}$ の巡回群であるから，中国式剰余定理から求める結果を得る．□

6.3.2 同型類を求める問題

例題 6.18 位数 15 の群の同型類を求めよ．

解答. G を位数 15 の群とする．G には 3-シロー部分群と，5-シロー部分群が存在する．まず，5-シロー部分群の個数は $1 + 5k$ なる形をしている 15 の約数であり，それは 1 しかない．よって，5-シロー部分群 P_5 はただ一つで，P_5 は G の正規部分群である．一方，3-シロー部分群の個数は $1 + 3l$ なる形をしている 15 の約数であり，やはり 1 しかない．よって，3-シロー部分群 P_3 もただ一つで，P_3 は G の正規部分群．

P_3 および P_5 は素数位数の巡回群であり，それらの生成元をそれぞれ a, b とおくと，$ab = ba$ が成り立つ．実際，P_3 は正規部分群ゆえ，$bP_3b^{-1} = P_3$．したがって，$bab^{-1} \in P_3$ となるが，もし $bab^{-1} = 1$ とすると $a = 1$ となるので矛盾．また，$bab^{-1} = a^2$ と仮定すると，両辺に右から a^{-1} 乗じて $a = b(ab^{-1}a^{-1})$ となるが，P_5 は正規部分群ゆえ，$a \in B$ となることが分かる．すると，$a \in A \cap B = \{1\}$ であるから $a = 1$ となり矛盾．したがって，$bab^{-1} = a$，すなわち，$ba = ab$ である．

さて，G において，a と b で生成される部分群を H とおくと，上の考察から H はアーベル群である．よって，補題 2.39 より，ab の位数は 15 となる．よって，$H = G \cong \mathbb{Z}/15\mathbb{Z}$ となる．すなわち，位数 15 の群は巡回群しかない．□

例題 6.19 $p \geq 3$ を素数とする．$|G| = 2p$ となる群 G の同型類の個数は 2 個であることを示せ．

解答. G の p-シロー部分群の個数は $1+pk$ なる形の $2p$ の約数であるから，1 個である．これを P とおくと，P は G の正規部分群である．次に，G の 2-シロー部分群の個数は奇数で，かつ $2p$ の約数ゆえ，1 個か p 個である．

(1) 2-シロー部分群の個数が 1 個のとき．

このとき，2-シロー部分群を Q とおくと，Q は G の正規部分群．P と Q は素数位数の巡回群であり，それらの生成元をそれぞれ a, b とおくと，$ab = ba$ である．実際，$aba^{-1} \in Q$ であるから，$aba^{-1} = 1$ または b となるが，$aba^{-1} = 1$ となったとすると，$b = 1$ となり矛盾．よって，$aba^{-1} = b$ となり，$ab = ba$ を得る．そこで，G において a と b で生成される部分群を H とおくと H はアーベル群であり，補題 2.39 より，ab の位数は $2p$ となる．よって，$H = G \cong \mathbb{Z}/2p\mathbb{Z}$ となる．すなわち，G は位数 $2p$ の巡回群である．

(2) 2-シロー部分群の個数が p 個のとき．

Q を G の任意の 2-シロー部分群として固定する．$P \cap Q = \{1_G\}$ に注意して，第 2 同型定理より

$$PQ/Q \cong P/(P \cap Q) \cong P$$

となるので，$|PQ| = |P||Q| = 2p$ を得る．すなわち，$PQ = G$ である．P と Q は素数位数の巡回群であり，それらの生成元をそれぞれ a, b とおく．P は G の正規部分群ゆえ，$bab^{-1} = a^l$ なる，$0 \le l \le p-1$ が存在する．このとき，

$$a^{l^2} = (a^l)^l = (bab^{-1})^l = ba^lb^{-1} = b^2ab^{-2} = a$$

となる．すなわち，$a^{l^2-1} = 1_G$ である．よって，$p|(l^2-1)$ となり，$p|(l-1)$ または $p|(l+1)$．今，$0 \le l \le p-1$ であるからこの条件を満たすものは $l = 1$ または $p-1$ のみである．もし $l = 1$ とすると，$ab = ba$ となり，(1) の議論と同様にして，$G \cong \mathbb{Z}/2p\mathbb{Z}$ であることが分かるが，位数 $2p$ の巡回群には，2-シロー部分群は一つしか存在しないのでこれは矛盾．よって，$l = p-1$ である．以上まとめると，G は位数 $2p$ の群で，2 つの元 a, b で生成されており，それらは

$$a^p = b^2 = 1, \quad bab^{-1} = a^{p-1} = a^{-1}$$

を満たす．このような群は存在し，それは p 次の正二面体群 D_p にほかならない（実際，$\sigma^i\tau^j \mapsto a^i b^j$ $(0 \leq i \leq p-1,\ 0 \leq \tau \leq 1)$ なる対応により同型写像 $D_p \to G$ が構成できる）．このとき，D_p の 2-シロー部分群は全部で

$$\{1, b\},\ \{1, ab\},\ \ldots,\ \{1, a^{p-1}b\}$$

の p 個ある．

したがって，G は $\mathbb{Z}/2p\mathbb{Z}$ か D_p に同型となる．D_p は非可換群であるから $D_p \not\cong \mathbb{Z}/2p\mathbb{Z}$ である．ゆえに求める結果を得る．□

例題 6.20 $p \geq 3$ を素数とする，$|G| = 3p$ となる群 G の同型類の個数は，

$$\begin{cases} 2, & p = 3 \text{ または } p \equiv 1 \pmod 3 \\ 1, & p \equiv 2 \pmod 3 \end{cases}$$

となることを示せ．

解答． まず，$p = 3$ のときは，$|G| = 9$ となり G はアーベル群である．ゆえに，$G \cong \mathbb{Z}/9\mathbb{Z}$ または $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ となり，G の相異なる同型類は二つ．以下，$p > 3$ とする．

G の p-シロー部分群の個数は $1 + pk$ なる形の $3p$ の約数であるから，1 個である．これを P とおくと，P は G の正規部分群である．次に，G の 3-シロー部分群の個数は $1 + 3l$ なる形の $3p$ の約数であるので，$p \equiv 2 \pmod 3$ であれば 1 個であり，$p \equiv 1 \pmod 3$ であれば 1 個か p 個である．

(1) $p \equiv 2 \pmod 3$ のとき．

このとき，3-シロー部分群は 1 個のみでそれを Q とおくと，Q は G の正規部分群．P と Q は素数位数の巡回群であり，それらの生成元をそれぞれ a, b とおくと，$ab = ba$ である．実際，$aba^{-1} \in Q$ であるから，$aba^{-1} = 1$ または b となるが，$aba^{-1} = 1$ となったとすると，$b = 1$ となり矛盾．よって，$aba^{-1} = b$ となり，$ab = ba$ を得る．そこで，G において a と b で生成される部分群を H とおくと H はアーベル群であり，補題 2.39 より，ab の位数は $3p$ となる．よって，$H = G \cong \mathbb{Z}/3p\mathbb{Z}$ となる．すなわち，G は位数 $3p$ の巡回

群である．

(2) $p \equiv 1 \pmod 3$ のとき．

(2-1) 3 シロー部分群の個数が 1 個のとき．このときは，(1) と同様にして，$G \cong \mathbb{Z}/3p\mathbb{Z}$ となることが分かる．

(2-2) 3 シロー部分群の個数が p 個のとき．Q を G の任意の 3-シロー部分群として固定する．$P \cap Q = \{1_G\}$ に注意して，第 2 同型定理より

$$PQ/Q \cong P/(P \cap Q) \cong P$$

となるので，$|PQ| = |P||Q| = 3p$ を得る．すなわち，$PQ = G$ である．P と Q は素数位数の巡回群であり，それらの生成元をそれぞれ a, b とおく．P は G の正規部分群ゆえ，$bab^{-1} = a^r$ なる，$0 \leq r \leq p-1$ が存在する．このとき，

$$\begin{aligned} a^{r^3} &= ((a^r)^r)^r = ((bab^{-1})^r)^r = (ba^r b^{-1})^r \\ &= (b^2ab^{-2})^r = b^2a^rb^{-2} = b^3ab^{-3} = a \end{aligned}$$

となる．すなわち，$a^{r^3-1} = 1_G$ である．よって，$p|(r^3-1)$ となり，$p|(r-1)$ または $p|(r^2+r+r)$．もし $p|(r-1)$ とすると，$0 \leq r \leq p-1$ であるから $r = 1$ となる．よって，$ab = ba$ となり，(1) の議論と同様にして $G \cong \mathbb{Z}/3p\mathbb{Z}$ となるが，この群には 3-シロー部分群は一つしか存在しないので矛盾．よって，$p|(r^2+r+1)$ でなければならない．実際，$p \equiv 1 \pmod 3$ のとき，このような r は法 p に関して丁度二つ存在する[47]．これらを r_1, r_2，$0 \leq r_1, r_2 \leq p-1$ とおくと，解と係数の関係から，$r_1 + r_2 \equiv -1$, $r_1r_2 \equiv 1 \pmod p$ となる．ここで，$r_1 \equiv r_2 \pmod p$ となったとすると，$r_1r_2 \equiv 1 \pmod p$ より，$r_1 \equiv \pm 1 \pmod p$ となるが，これは $r_1 + r_2 \equiv -1 \pmod p$ に矛盾．よって，$r^2 + r + 1 = 0 \pmod p$ は相異なる二つの解を持つ．また，$i = 1, 2$ に対して，$r_i \equiv 1 \pmod p$ となったとすると，$p|3$ となり，これは $p > 3$ に矛盾．また，$p|(r_i^2 + r_i + 1)$ であるから $p|r_i$ となることはない．したがって，$[r_i]_p \in (\mathbb{Z}/p\mathbb{Z})^\times$ である．以上をまとめると，G は位数 $3p$ の群で二つの元 a, b で生成されており，それらは

$$a^p = b^3 = 1, \quad bab^{-1} = a^{r_i}, \quad (r_i^3 \equiv 1,\ r_i \not\equiv 0, 1 \pmod p)$$

[47] $r^2 + r + 1 = 0 \pmod p$ は，両辺を 4 倍して平方完成することにより，$(2r+1)^2 \equiv -3 \pmod p$ と同値である．$p \equiv 1 \pmod 3$ のとき，-3 は平方剰余であり，$x^2 \equiv -3 \pmod p$ は法 p に関して重複度も込めて二つの解を持つ．これらを x_1, x_2 とおけば，$r = (x_1 - 1)/2$, $(x_2 - 1)/2$ となる．

を満たす．このような群は存在し，それはメタ巡回群 $G_{p,3}(r_i)$ にほかならない．[48)] このとき，$G_{p,3}(r_i)$ の 3-シロー部分群は全部で

$$\{1, b, b^2\},\ \{1, ab, a^{1+r_i}b^2\},\ \ldots\ \{1, a^{p-1}b, a^{(p-1)(1+r_i)}b^2\}$$

の p 個ある．

48) 実際，例 5.36 で考えた $G_{p,3}(r_i)$ の二つの生成元 a, b をここでのものと区別してそれぞれ c, d とおくと，$c^i d^j \mapsto a^i b^j$ $(0 \le i \le p-1,\ 0 \le \tau \le 2)$ なる対応により同型写像 $G_{p,3}(r_i) \to G$ が構成できる．

最後に，$G_{p,3}(r_1)$ と $G_{p,3}(r_2)$ が同型であることを示そう．今，$G_{p,3}(r_1)$ と $G_{p,3}(r_2)$ を区別するために，$G_{p,3}(r_2)$ における上記の a, b を便宜的に α, β と書く．このとき，写像 $f : G_{p,3}(r_1) \to G_{p,3}(r_2)$ を

$$f(a^j b^i) = \alpha^j \beta^{2i}$$

によって定める．すると，任意の $a^{j_1}b^{i_1}, a^{j_2}b^{i_2} \in G_{p,3}(r_1)$ に対して，

$$f(a^{j_1}b^{i_1} \cdot a^{j_2}b_{i_2}) = f(a^{j_1+r_1^{i_1}j_2}b^{i_1+i_2}) = \alpha^{j_1+r_1^{i_1}j_2}\beta^{2(i_1+i_2)}$$

であり，$r_2^2 \equiv -r_2 - 1 \equiv r_1 \pmod p$ に注意すれば，

$$\begin{aligned} f(a^{j_1}b^{i_1})f(a^{j_2}b^{i_2}) &= \alpha^{j_1}\beta^{2i_1}\alpha^{j_2}\beta^{2i_2} \\ &= \alpha^{j_1+r_2^{2i_1}j_2}\beta^{2(i_1+i_2)} = \alpha^{j_1+r_1^{i_1}j_2}\beta^{2(i_1+i_2)} \end{aligned}$$

となり，f が群準同型写像であることが分かる．

さて，α と β は $G_{p,3}(r_2)$ の生成元であり，$f(a) = \alpha$, $f(b^2) = \beta^4 = \beta$ であるから f は全射である．さらに，$f(a^{j_1}b^{i_1}) = f(a^{j_2}b^{i_2})$ とすると，$\alpha^{j_1}\beta^{2i_1} = \alpha^{j_2}\beta^{2i_2}$ であるから，$j_1 \equiv j_2 \pmod p$, $2i_1 \equiv 2i_2 \pmod p$ となり，2 は法 p について可逆ゆえ，$i_1 \equiv i_2 \pmod p$ を得る．したがって，$a^{j_1}b^{i_1} = a^{j_2}b^{i_2}$ となり，f は単射である．よって同型写像である．

以上より，$p \equiv 1 \pmod 3$ のとき G は $\mathbb{Z}/3p\mathbb{Z}$ か $G_{p,3}(r_1)$ に同型となる．$G_{p,3}(r_1)$ は非可換群であるから $G_{p,3}(r_1) \not\cong \mathbb{Z}/3p\mathbb{Z}$ である．ゆえに求める結果を得る．□

6.4 問題

問題 6.1 p を素数とし，F を $q = p^m$（$m > 1$）個の元からなる体

とする．$n \geq 1$ を自然数とする．

(1) $\mathrm{GL}(n,F)$ の位数を求めよ．

(2) $\mathrm{SL}(n,F)$ の位数を求めよ．

(3) $\mathrm{GL}(n,F)$ の元で，対角成分がすべて 1 であるような上三角行列全体を U とおく．このとき，U は $\mathrm{GL}(n,F)$，および $\mathrm{SL}(n,F)$ の p-シロー部分群であることを示せ．

解答. (1) 体 F 上の n 次元ベクトル空間を V とし固定する．V の基底を一つとって $(\boldsymbol{v}_1,\boldsymbol{v}_2,\ldots,\boldsymbol{v}_n)$ とおく．V の任意の元 $\boldsymbol{x}$ は一意的に $x_1\boldsymbol{v}_1+\cdots+x_n\boldsymbol{v}_n$ と表せるので，$|V|=q^n$ である．一方，V の基底全体のなす集合を $\mathcal{B}$ とおく．基底の変換を考えると，写像 $f:\mathrm{GL}(n,F)\to\mathcal{B}$ を $A\mapsto(\boldsymbol{v}_1\,\boldsymbol{v}_2\,\ldots\,\boldsymbol{v}_n)A$ によって定めれば，f が全単射であることが分かる．つまり，$|\mathrm{GL}(n,F)|=|\mathcal{B}|$ である．したがって，V の基底がどれだけあるかを調べればよい．

一般に，V の基底 $(\boldsymbol{w}_1,\boldsymbol{w}_2,\ldots,\boldsymbol{w}_n)$ を $\boldsymbol{w}_1$ から順に構成することを考える．すると，$\boldsymbol{w}_1$ の取り方は $\boldsymbol{w}_1$ が一次独立になるような場合の数だけあり，それは $\boldsymbol{w}_1$ が $\boldsymbol{0}$ 以外の場合だから，全部で q^n-1 通り．次に，$\boldsymbol{w}_2$ の取り方は，$\boldsymbol{w}_1,\boldsymbol{w}_2$ が一次独立になるような場合の数だけある．ここで，$\boldsymbol{w}_1,\boldsymbol{w}_2$ が一次従属になるような場合の数は，$\boldsymbol{w}_2$ が $\boldsymbol{w}_1$ のスカラー倍になっている場合の数で全部で q 通り．したがって，求める場合の数は q^n-q 通り．以下同様にして，$\boldsymbol{v}_1,\ldots,\boldsymbol{v}_i$ が定まっているときに，$\boldsymbol{v}_{i+1}$ の取り方は，$\boldsymbol{v}_{i+1}$ が $\boldsymbol{v}_1,\ldots,\boldsymbol{v}_i$ の一次結合とはならないような場合の数で，全部で q^n-q^i 通りである．ゆえに，

$$
\begin{aligned}
|\mathrm{GL}(n,F)| &= (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})\\
&= q^{\frac{n(n-1)}{2}}(q^n-1)(q^{n-1}-1)\cdots(q-1)
\end{aligned}
$$

を得る．

(2) 行列式を与える写像 $\det:\mathrm{GL}(n,F)\to F^\times$ は全射準同型写像であり，核は $\mathrm{SL}(n,F)$ にほかならない．よって，$|\mathrm{GL}(n,F)|/|\mathrm{SL}(n,F)|=|\mathrm{GL}(n,F)/\mathrm{SL}(n,F)|=|F^\times|=q-1$ より，

$$
|\mathrm{SL}(n,F)| = q^{\frac{n(n-1)}{2}}(q^n-1)(q^{n-1}-1)\cdots(q^2-1)
$$

となる．

(3) (1) より，$|\mathrm{GL}(n,F)|$ を割り切る p の最大冪は $q^{\frac{n(n-1)}{2}}$ であり，$|U|=q^{\frac{n(n-1)}{2}}$ となることは明らかであるから，U は $\mathrm{GL}(n,F)$ の p-シロー部分群である．さらに，(2) より $|\mathrm{SL}(n,F)|$ を割り切る p の最大冪も $q^{\frac{n(n-1)}{2}}$ であり，U は $\mathrm{SL}(n,F)$ の部分群でもあるから，U は $\mathrm{SL}(n,F)$ の p-シロー部分群でもある．□

問題 6.2 位数 35 の群の同型類の個数を求めよ．

解答．G を位数 35 の群とする．G の 5 シロー部分群 P_5，7 シロー部分群 P_7 の個数はともに一つであり，それらは G の正規部分群である．a, b をそれぞれ P_5，P_7 の生成元とする．このとき，$bab^{-1}=a^l$，$(0 \leq l \leq 4)$ と書ける．$l=0$ とすると $a=1_G$ となり矛盾．$2 \leq l \leq 4$ とすると，$bab^{-1}=a^l$ より $b(ab^{-1}a^{-1})=a^{l-1}$ を得る．よって，$a^{l-1} \in A \cap B$ である．$a^{l-1} \neq 1_G$ であり，a^{l-1} の位数は 5 でなければならないが，5 は 7 の約数ではないので $a^{l-1} \in B$ となることはない．したがって，$bab^{-1}=a$ となり，G はアーベル群である．

よって，補題 2.39 より，ab の位数は 35 となる．よって，$G \cong \mathbb{Z}/35\mathbb{Z}$ となる．すなわち，位数 35 の群は巡回群しかないので求める同型類の個数は 1 個である．□

問題 6.3 $\mathfrak{S}_4$ のシロー部分群をすべて求めよ．

解答．$|\mathfrak{S}_4|=24=3\times 8$ であるから，$\mathfrak{S}_4$ には 3 シロー部分群と 2 シロー部分群が存在する．

(1) 3 シロー部分群について．

$\mathfrak{S}_4$ の 3 シロー部分群の個数は $1+3k$ なる形の 24 の約数であるから，1 または 4 個である．3 次の巡回置換を考えることにより，

$$P_3=\langle(1\,2\,3)\rangle,\quad \langle(1\,2\,4)\rangle,\quad \langle(1\,3\,4)\rangle,\quad \langle(2\,3\,4)\rangle$$

の 4 つであることが分かる．

(2) 2 シロー部分群について．

$\mathfrak{S}_4$ の 2 シロー部分群の個数は奇数である 24 の約数である．よって，1 個か 3 個．まず，$\mathfrak{S}_4$ に含まれる位数 8 の部分群として 4 次の

正二面体群

$$D_4 = \{1,\ (1\,3),\ (2\,4),\ (1\,2)(3\,4),\ (1\,4)(2\,3),\ (1\,3)(2\,4),\ (1\,2\,3\,4),\ (1\,4\,3\,2)\}$$

がある．そこで，この群と共役な部分群を考察すると，

$$(3\,4)D_4(3\,4) = \{1,\ (1\,4),\ (2\,3),\ (1\,2)(3\,4),\ (1\,4)(2\,3),\ (1\,3)(2\,4),\ (1\,2\,4\,3),\ (1\,3\,4\,2)\}$$

$$(2\,3)D_4(2\,3) = \{1,\ (1\,2),\ (3\,4),\ (1\,2)(3\,4),\ (1\,4)(2\,3),\ (1\,3)(2\,4),\ (1\,3\,2\,4),\ (1\,4\,2\,3)\}$$

が得られる．よって，$\mathfrak{S}_4$ の 2 シロー部分群はこれら 3 個である．□

問題 6.4 東京理科大学の前身である東京物理学校は 1883 年に設立された．そこで，位数 1883 の群の同型類の個数を求めよ．

西暦に関して，自分の誕生年や記念になる年を位数に持つ群の同型類の個数を求めてみよ（場合によっては恐ろしく複雑になることもあるので，無理せず気楽に考えてみてください）．

解答．G を位数が 1883 の群とする．1883 を素因数分解すると，$1883 = 7 \times 269$ となる．簡単な考察から，G は 7 シロー部分群と 269 シロー部分群の個数は各 1 個であることが分かる．それらをそれぞれ P_7，P_{269} とおくと，これらは正規部分群で，かつ素数位数の巡回群である．a, b をそれぞれ P_7，P_{269} の生成元とすれば，上述の問題における議論と同様にして，$ab = ba$ であることもわかる．よって，G はアーベル群である．以上より，$G \cong \mathbb{Z}/1883\mathbb{Z}$ を得る．したがって，求める同型類の個数は 1 個である．□

付録

初等整数論からの準備

この節では，初等整数論の基本的な定理で本書でもよく扱うものを解説する．群論に限らず，代数学を勉強する際にしばしば必要とされることでもあるので一度身に付けておかれるとよいと思う．

定理 A.1（**剰余の定理**）$n \geq 1$ を自然数とする．このとき，任意の整数 $a \in \mathbb{Z}$ に対して，ある整数 $q, r \in \mathbb{Z}$ で，

$$a = nq + r, \quad 0 \leq r < n$$

となるものが存在する．

証明. 実数直線上に n の整数倍の点をとる．すると，任意の $a \in \mathbb{Z}$ に対して，$qn \leq a < (q+1)n$ となる q が一意的に存在する．このとき，$r = a - qn$ とおけばよい．□

0 でない二つの整数 a, b に対して，a と b の最大公約数を $\gcd(a, b)$ とかく．$\gcd(a, b) = 1$ のとき，a と b は**互いに素** (relatively prime) という．

定理 A.2 0 でない整数 a, b, q, r に対して，$a = bq + r$ なる関係があるとする．このとき，

$$\gcd(a, b) = \gcd(b, r).$$

証明. $d = \gcd(a, b)$ とおくと，$d|a$ かつ $d|b$ であり，$r = a - bq$ であ

るから $d|r$ となる．よって，d は b と r の公約数となり，$d \leq \gcd(b, r)$ を得る．同様に逆向きの不等号も示せるので求める結果を得る．□

定理 A.3（ユークリッドの互除法） $a_1 > a_2 > 0$ なる自然数 a_1, a_2 に対して，剰余の定理を繰り返して適用することにより以下のようになったとする．

$$\begin{cases} a_1 = a_2 q_1 + a_3, & 0 < a_3 < a_2 \\ a_2 = a_3 q_2 + a_4, & 0 < a_4 < a_3 \\ \vdots \qquad \vdots \\ a_{n-1} = a_n q_{n-1} + a_{n+1}, & 0 < a_{n+1} < a_n \\ a_n = a_{n+1} q_n \end{cases} \tag{A.1}$$

このとき，$\gcd(a_1, a_2) = a_{n+1}$ である．

証明. 定理 A.2 を繰り返し用いればよい．□

定理 A.4 $\gcd(a, b) = 1$ なる整数 a, b に対して，ある整数 x, y で，$ax + by = 1$ なるものが存在する．

証明. 一般に，$\gcd(|a|, |b|) = \gcd(a, b)$ であり，$|a| = \pm a$，$|b| = \pm b$ であるから，はじめから a, b は自然数であると仮定してよい．さらに，必要であれば a と b を入れ換えることで，$a > b > 0$ としても一般性を失わない．そこで，$a_1 = a$, $a_2 = b$ とおいて剰余の定理を繰り返すことで (A.1) なる式を作ることを考える．各操作における余りの列は真に減少する自然数列であるから，いずれ，ある n で $a_{n+1} = 1$ となるものが取れる．このとき，(A.1) を変形すると

$$\begin{cases} a_3 = -a_2 q_1 + a_1, & 0 < a_3 < a_2 \\ a_4 = -a_3 q_2 + a_2, & 0 < a_4 < a_3 \\ \vdots \qquad \vdots \\ a_n = -a_{n-1} q_{n-2} + a_{n-2}, & 0 < a_n < a_{n-1} \\ a_{n+1} = -a_n q_{n-1} + a_{n-1}, & 0 < a_{n+1} < a_n \end{cases}$$

となる．このとき，一番下の式にある a_n に，その一つ上の式を代入

することで $a_{n+1}(=1)$ が a_{n-1} と a_{n-2} の整数係数の一次結合として表されることが分かる．この操作を逐次繰り返すことにより求める結果を得る．□

定義 A.5（オイラー関数） $n \geq 1$ を自然数とする．$1, 2, \ldots, n$ のうち，n と互いに素であるようなものの個数を $\varphi(n)$ と書く．例えば，$\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(6) = 2$ である．

このとき，関数 $\varphi : \mathbb{N} \to \mathbb{N}$ を**オイラー関数** (Euler's function) という．

注意 A.6 $n \geq 1$ を自然数とするとき，$\varphi(n)$ は次のようにいい換えることもできる．

(1) $\varphi(n)$ は

$$\frac{1}{n},\ \frac{2}{n},\ \ldots,\ \frac{n}{n}$$

のうち，既約分数であるものの個数である．

(2) $x \equiv y \pmod{n}$ とするとき，簡単な考察から，

$$\gcd(x, n) = 1 \Longleftrightarrow \gcd(y, n) = 1$$

であることが分かる．したがって，$A \subset \mathbb{Z}$ を $\mathbb{Z}/n\mathbb{Z}$ の任意の完全代表系とするとき，

$$\varphi(n) = |\{a \in A \mid \gcd(a, n) = 1\}|.$$

定理 A.7 オイラー関数について以下が成り立つ．p を素数とする．

(1) 任意の $e \in \mathbb{N}$ に対して，$\varphi(p^e) = p^{e-1}(p-1)$.

(2) $m, n \in \mathbb{N}$ を互いに素な自然数とするとき，$\varphi(mn) = \varphi(m)\varphi(n)$.

証明. (1) $1, 2, \ldots, p^e$ のうち，p^e と互いに素な自然数は，p と互いに素な自然数にほかならない．つまり，$1, 2, \ldots, p^e$ のうち，p の倍数でないものの個数を求めればよい．すると，p の倍数は全部で

$$p,\ 2p,\ \ldots,\ p^{e-1}p$$

の p^{e-1} 個ある．よって，$\varphi(p^e) = p^{e-1}(p-1)$ である．

(2) まず，

$$A := \{am + bn \mid 0 \leq a \leq n-1,\ 0 \leq b \leq m-1\}$$

を考える．A は法 mn に関する完全代表系である．実際，a_1m+b_1n, $a_2m+b_2n \in A$ として

$$a_1m + b_1n \equiv a_2m + b_2n \pmod{mn}$$

と仮定すると，$b_1n \equiv b_2n \pmod{m}$ となる．一方，m と n は互いに素であるから，$mx + ny = 1$ となる整数 x, y が存在する．このとき，$ny \equiv 1$ である．そこで，$b_1n \equiv b_2n \pmod{m}$ の両辺に y を乗じて，$b_1 \equiv b_2 \pmod{n}$ を得る．これより，$b_1 = b_2$ であることが分かる．同様にして $a_1 = a_2$ も得られる．したがって，A の相異なるどの二つの元も法 mn で合同でなく，$|A| = mn$ であることから，A は法 mn に関する完全代表系となることが分かる．

さて，$am + bn \in A$ に対して，$\gcd(m, n) = 1$ に注意して，

$$\begin{aligned}\gcd(am+bn, mn) = 1 \Longleftrightarrow{}& \gcd(am+bn, m) = 1 \\ & \text{かつ } \gcd(am+bn, n) = 1 \\ & \gcd(bn, m) = 1 \text{ かつ } \gcd(am, n) = 1 \\ & \gcd(b, m) = 1 \text{ かつ } \gcd(a, n) = 1\end{aligned}$$

となることが分かる．したがって，A の元で mn と互いに素なものは

$$\{am+bn \mid 0 \leq a \leq n-1,\ 0 \leq b \leq m-1,\ \gcd(a, n) = 1,\ \gcd(b, m) = 1\}$$

であり，これらは全部で $\varphi(m)\varphi(n)$ 個ある．すなわち，$\varphi(mn) = \varphi(m)\varphi(n)$ である．□

参考文献

[1] 浅野 啓三，永尾 汎：『群論』，岩波全書，岩波書店 (1965).
[2] 北村 泰一：『数論入門』，槇書店 (1986).
[3] 倉田令二朗：『平方剰余の相互法則』日本評論社 (1992).
[4] 近藤 武：『群論』，岩波基礎数学選書，岩波書店 (1991).
[5] 鈴木 通夫：『群論 上・下』，岩波書店 (1978).
[6] 高木 貞治：『初等整数論講義』，共立出版 (1971).
[7] 新妻 弘，木村哲三:『群・環・体入門』，共立出版 (1999).
[8] 松坂 和夫：『代数系入門』，岩波書店 (1976).
[9] 宮西 正宜:『代数学 1』，裳華房 (2010).
[10] 矢野 健太郎編，東京理科大学数学教育研究所編集：『数学小辞典 第 2 版』，共立出版 (2010).
[11] 山本 芳彦：『数論入門』，岩波書店 (2003).
[12] 横井 英夫，硲野敏博：『代数演習』，サイエンス社 (1989).
[13] 渡辺 哲雄：『群論演習』，槇書店 (1987).
[14] D. L. Johnson：*Presentation of groups*, Cambridge University Press (1997).
[15] W. Magnus：Über n-dimensinale Gittertransformationen, *Acta Math.* 64, pp.353–367 (1935).
[16] L. Sylow：Théorèmes sur les groupes de substitutions, *Math. Ann.* 5, pp.584–594 (1872).

※ iv ページに掲載した写真は，wikipedia より引用した，パブリック・ドメインとされているものです．

索　引

著 者 紹 介

佐藤 隆夫（さとう たかお）

1979 年生まれ，横浜市出身．
2006 年 3 月，東京大学大学院数理科学研究科 数理科学専攻博士課程修了．
現在，東京理科大学 理学部第二部数学科講師．
専門は代数的位相幾何学．博士（数理科学）．

大学数学 スポットライト・シリーズ①

シローの定理

2015 年 4 月 30 日　　初版第 1 刷発行

著 者　　佐 藤 隆 夫

発行者　　小 山 透

発行所　　株式会社 **近代科学社**

〒 162-0843　東京都新宿区市谷田町 2-7-15
電 話　03-3260-6161　振 替　00160-5-7625
http://www.kindaikagaku.co.jp

藤原印刷　　ISBN978-4-7649-0478-1

定価はカバーに表示してあります．